MCT USE ONLY. STUDENT USE PROHIBITED

# Module 6

## Implementing a Group Policy Infrastructure

### Contents:

**Lesson 1:** Understand Group Policy **6-4**

**Lesson 2:** Implement GPOs **6-20**

**Lab A:** Implement Group Policy **6-29**

**Lesson 3:** Manage Group Policy Scope **6-33**

**Lab B:** Manage Group Policy Scope **6-54**

**Lesson 4:** Group Policy Processing **6-59**

**Lesson 5:** Troubleshoot Policy Application **6-67**

**Lab C:** Troubleshoot Policy Application **6-75**

# Module Overview

• Understand Group Policy
• Implement GPOs
• Manage Group Policy Scope
• Group Policy Processing
• Troubleshoot Policy Application

In Module 1, you learned that Active Directory® Domain Services (AD DS) provides the foundational services of an identity and access solution for enterprise networks running Windows®, and that AD DS also supports the management and configuration of even the largest, most complex networks. In Modules 2 through 5, you learned how to administer AD DS security principals: users, groups, and computers. Now, you will examine the management and configuration of users and computers by using Group Policy. Group Policy provides an infrastructure within which settings can be defined centrally and deployed to users and computers in the enterprise.

In an environment managed by a well-implemented Group Policy infrastructure, little or no configuration needs to be made by directly touching a desktop. The entire configuration is defined, enforced, and updated by using the settings in Group Policy objects (GPOs) that affect a portion of the enterprise as broad as an entire site or a domain, or as narrow as a single organizational unit (OU) or a group. In this module, you will learn what Group Policy is, how it works, and how best to implement it in your organization. Several subsequent modules will apply Group Policy to specific management tasks such as security configuration, software deployment, password policy, and auditing.

### Objectives

After completing this module, you will be able to:

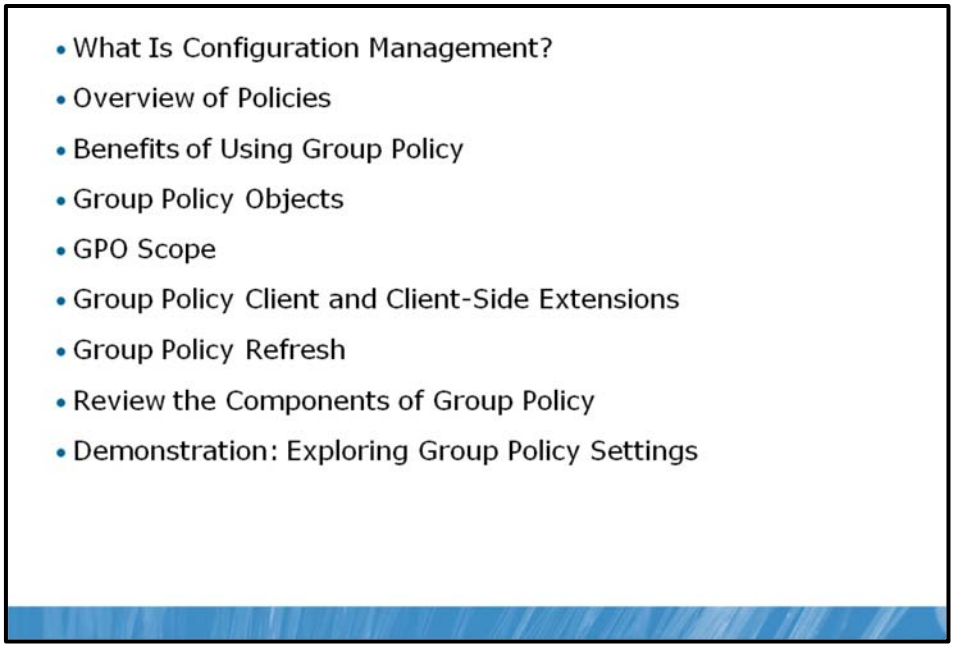
- Describe the components and technologies that comprise the Group Policy framework.
- Implement GPOs.
- Configure and understand a variety of policy setting types.
- Understand and configure Group Policy preferences.
- Scope GPOs by using links, security groups, Windows® Management Instrumentation filters, loopback processing, and preference targeting.

MCT USE ONLY. STUDENT USE PROHIBITED

- Describe how GPOs are processed.
- Locate the event logs containing Group Policy–related events and troubleshoot Group Policy application.

MCT USE ONLY. STUDENT USE PROHIBITED

# Lesson 1
# Understand Group Policy


What Is Configuration Management?
Overview of Policies
Benefits of Using Group Policy
Group Policy Objects
GPO Scope
Group Policy Client and Client-Side Extensions
Group Policy Refresh
Review the Components of Group Policy
Demonstration: Exploring Group Policy Settings

A Group Policy infrastructure has several moving parts. You need to understand not only what each part does, but also how they work together and why you might want to assemble them in various configurations. In this lesson, you will get a comprehensive overview of Group Policy: its components, its functions, and its inner workings.

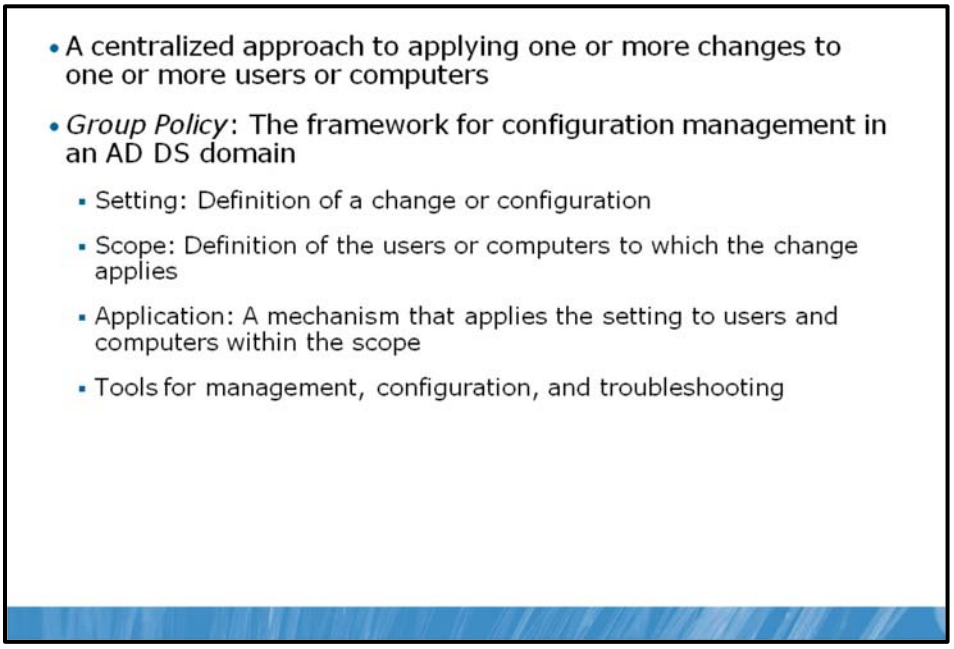
### Objectives

After completing this lesson, you will be able to:

- Identify the business drivers for configuration management.
- Understand the core components and terminology of Group Policy.
- Explain the fundamentals of Group Policy processing.

MCT USE ONLY. STUDENT USE PROHIBITED

## What Is Configuration Management?


• A centralized approach to applying one or more changes to one or more users or computers
• *Group Policy*: The framework for configuration management in an AD DS domain
▪ Setting: Definition of a change or configuration
▪ Scope: Definition of the users or computers to which the change applies
▪ Application: A mechanism that applies the setting to users and computers within the scope
▪ Tools for management, configuration, and troubleshooting

If you have only one computer in your environment—at home, for example—and you need to modify the desktop background, there are several ways to do that. Most people would probably open Personalization from Control Panel and make the change by using the Windows interface. That works well for one user, but may become tedious if you want to make the change across multiple users. Say, for example, that you want the same background for yourself and your family. You have to make the change multiple times, and then if you ever change your mind and want to change the background yet again, you have to return to each user's profile and make the change. Implementing the change and maintaining a consistent environment becomes even more difficult across multiple computers.

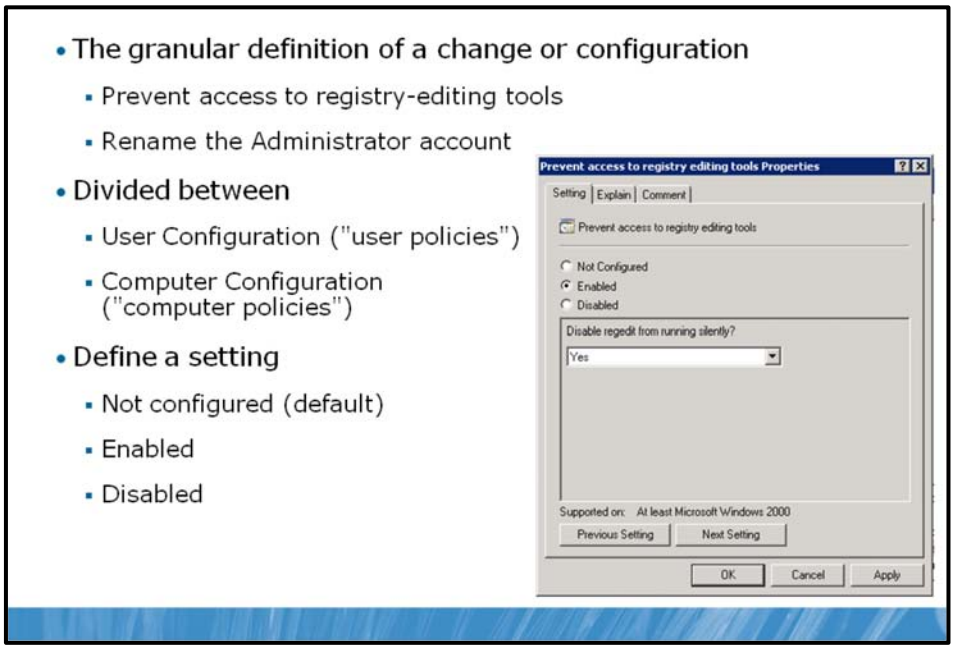
Configuration management is a centralized approach to applying one or more changes to one or more users or computers. If you remember that, everything else will be easier to understand. The key elements of configuration management are:

- A centralized definition of a change, which is known as a setting. The setting brings a user or a computer to a desired state of configuration.
- A definition of the user(s) or computer(s) to whom the change applies, which is known as the scope of the change.
- A mechanism or process that ensures that the setting is applied to users and computers within the scope, which is known as the application.

Group Policy is a framework within Windows—with components that reside in Active Directory, on domain controllers, and on each Windows server and client—that enables you to manage configuration in an AD DS domain. As we turn our attention to Group Policy, which can become very complex, always remember that everything boils down, in the end, to just these few basic elements of configuration management.

MCT USE ONLY. STUDENT USE PROHIBITED

## Overview of Policies




The most granular component of the Group Policy is an individual policy setting, also known simply as a policy that defines a specific configuration change to apply. For example, a policy setting exists that prevents a user from accessing registry-editing tools. If you define that policy setting and apply it to the user, the user will be unable to run tools such as Regedit.exe. Another policy setting is available that you can use to rename the local Administrator account. You can use this policy setting to rename the Administrator account on all user desktops and laptops.

These two examples illustrate an important point: that some policy settings affect a user, regardless of the computer to which the user logs on, and other policy settings affect a computer, regardless of which user logs on to that computer. Policy settings such as the setting that prevents access to registry-editing tools are often referred to as *user* configuration settings or user settings. Policy settings such as the one that disables the Administrator account and similar settings are often referred to as computer configuration settings or computer settings. You will also hear these referred to as user policies and computer policies. The terminology used in the industry is not exact.

There are various policy settings that can be managed by Group Policy, and the framework is extensible. So, in the end, you could manage just about anything with Group Policy.

To define a policy setting, double-click it.

The policy setting **Properties** dialog box appears.

A policy setting can have three states: **Not Configured**, **Enabled**, and **Disabled**.

In a new GPO, every policy setting is set to **Not Configured**. This means that the GPO will not modify the existing configuration of that particular setting for a user or computer. If you enable or disable a policy setting, a change will be made to the configuration of users and computers to which the GPO is applied.

The effect of the change depends on the policy setting. For example, if you enable the **Prevent Access To Registry Editing Tools** policy setting, users will be unable to launch the Regedit.exe Registry Editor. If

MCT USE ONLY. STUDENT USE PROHIBITED

you disable the policy setting, you ensure that users can launch the Registry Editor. Notice the double negative in this policy setting: You disable a policy that prevents an action, so you allow the action.

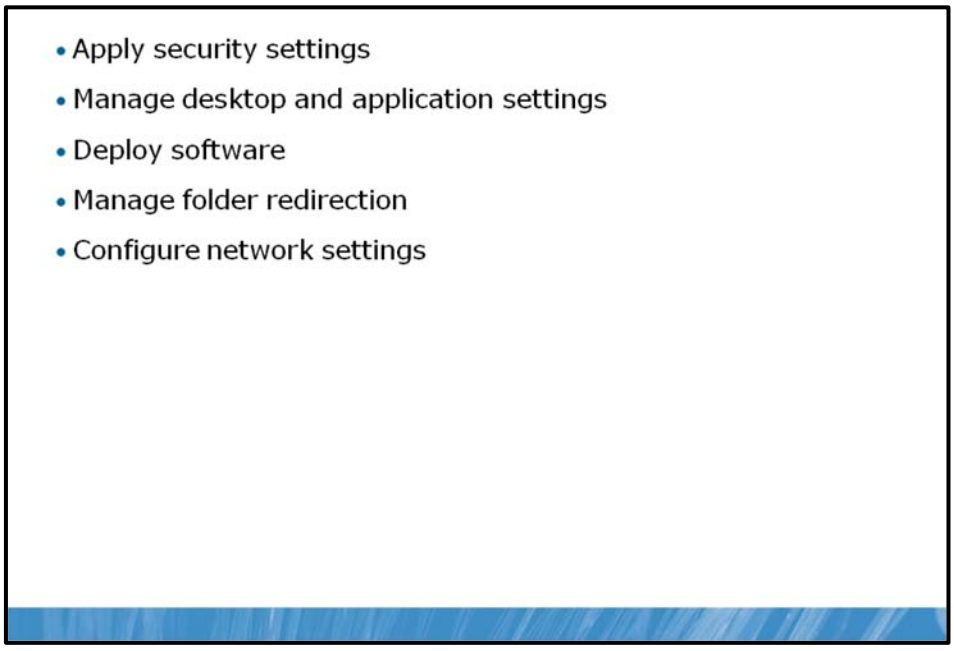
Some policy settings bundle several configurations into one policy and might require additional parameters. In the screenshot above, you can see that by enabling the policy to restrict registry editing tools, you can also define whether registry files can be merged into the system silently by using regedit /s.

**Note** Many policy settings are complex, and the effect of enabling or disabling them might not be immediately clear. Also, some policy settings affect only certain versions of Windows. Be sure to review a policy setting's explanatory text in the Group Policy Management Editor (GPME) detail pane or on the Explain tab in the policy setting's Properties dialog box. In addition, always test the effects of a policy setting and its interactions with other policy settings before deploying a change in the production environment.

You will explore policy settings and how to manage them in Lesson 3.

MCT USE ONLY. STUDENT USE PROHIBITED

## Benefits of Using Group Policy


• Apply security settings
• Manage desktop and application settings
• Deploy software
• Manage folder redirection
• Configure network settings

Group Policies are a very powerful administrative tool. You can use them to enforce various types of settings to a large number of users and computers. Because they can be applied to various levels from local to domain, you can also focus these settings very precisely.

Primarily, you can use Group Policies to configure settings that you do not want users to configure. Also, Group Policies are usually used to standardize desktop environments on all the computers in an organizational unit or whole organization. You also can use Group Policies to provide additional security and some advanced system settings.

Most often Group Policies are used for following purposes.

### Apply Security Settings

In Windows Server 2008 R2, GPOs include a large number of security-related settings that you can apply to both users and computers. For example, you can enforce settings for Windows Firewall and configure Auditing, Encrypting File System (EFS) policies and other security settings. You can also configure full set of user rights assignments.

### Manage Desktop and Application Settings

You can use a Group Policy to provide a consistent desktop and application environment to all users in your organization Using GPOs, it is possible to configure each setting that affects the look and feel of user environment and also to configure settings for some applications that support GPOs.

### Deploy Software

Group Policies can also be used to deploy software for users or computers. All software that is provided in the .msi format can be deployed by using Group Policy. You can enforce automatic software installation or you can let your users decide if they want the software to be deployed to their machines or not.

MCT USE ONLY. STUDENT USE PROHIBITED

### Manage Folder Redirection

With Folder Redirection, you can easily manage and back up data. By redirecting folders, you can ensure that users have access to their data regardless of the computer that they use to log on. Also, you can centralize all users' data to one place on the network server, while still providing the user an experience similar to storing these folders on their computers.

### Configure Network Settings.

Using Group Policies, you can configure various network settings on client computers. For example, you can enforce settings for wireless networks to allow users to connect only to specific SSIDs and with pre-defined authentication and encryption settings. You can also deploy policies that apply to wired network settings as well as configure client side of services such as Network Access Protection

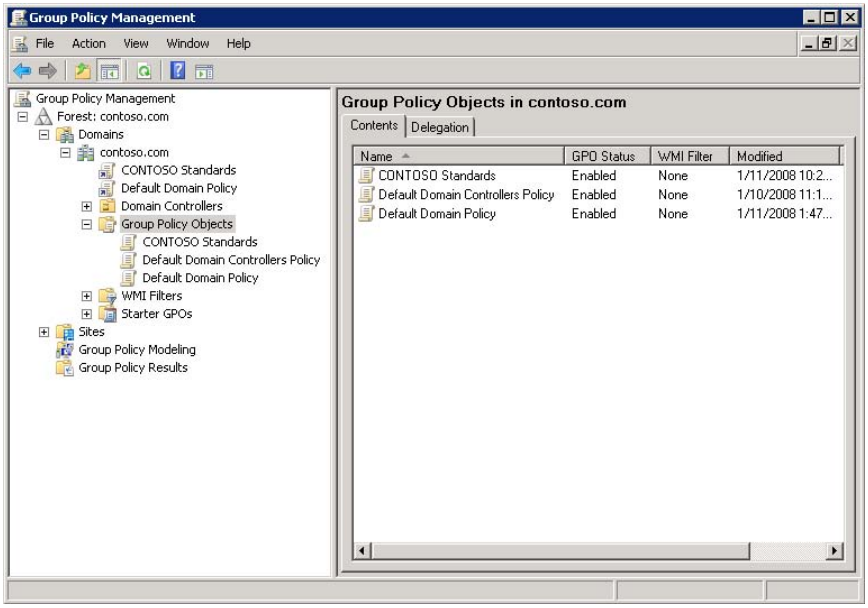
MCT USE ONLY. STUDENT USE PROHIBITED

## Group Policy Objects

- Container for one or more policy settings
- Managed with the GPMC
- Stored in Group Policy Objects container
- Edited with the GPME
- Applied to a specific level in AD DS hierarchy

Policy settings are defined and exist within a *GPO*. A GPO is an object that contains one or more policy settings and thereby applies one or more configuration settings for a user or a computer.

GPOs can be managed in Active Directory by using the Group Policy Management console (GPMC), shown here:



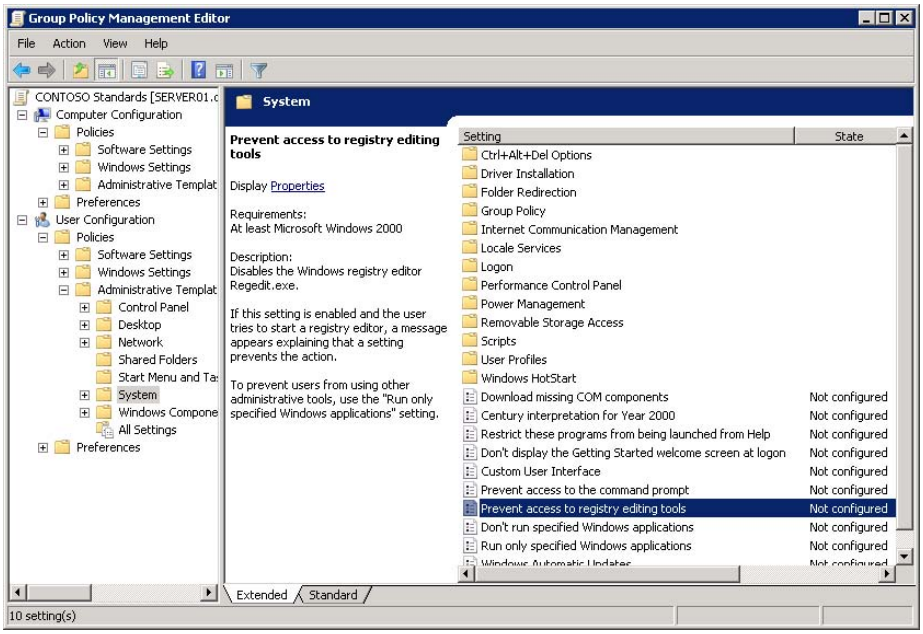

GPOs are displayed in a container named Group Policy Objects.

To create a new GPO in a domain, right-click the **Group Policy Objects** container, and then click **New**.

MCT USE ONLY. STUDENT USE PROHIBITED

To modify the configuration settings in a GPO, right-click the GPO, and then click **Edit**.

The GPO opens in the GPME snap-in, formerly known as the Group Policy Object Editor (GPO Editor), shown here:



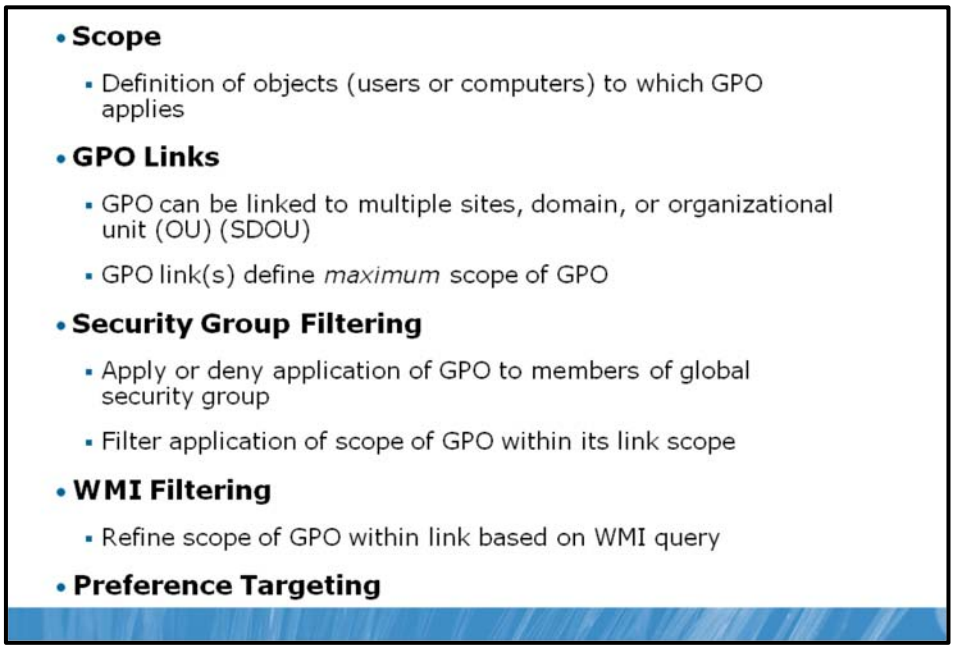

The GPME displays the thousands of policy settings available in a GPO in an organized hierarchy that begins with the division between computer settings and user settings, the Computer Configuration node and the User Configuration node. The next levels of the hierarchy are two nodes called Policies and Preferences. You will learn about the difference between these two nodes as this lesson progresses. Drilling deeper into the hierarchy, you will see that the GPME displays folders, which are also called nodes or policy setting groups. Within the folders are the policy settings themselves. The Prevent Access To Registry Editing Tools option is selected in the screenshot shown here.

The GPO must be applied to domain, site, or OU in the AD DS hierarchy for the settings within the object to take effect.

You will learn how to implement and manage GPOs in Lesson 2.

MCT USE ONLY. STUDENT USE PROHIBITED

## GPO Scope


Scope
Definition of objects (users or computers) to which GPO applies
GPO Links
GPO can be linked to multiple sites, domain, or organizational unit (OU) (SDOU)
GPO link(s) define maximum scope of GPO
Security Group Filtering
Apply or deny application of GPO to members of global security group
Filter application of scope of GPO within its link scope
WMI Filtering
Refine scope of GPO within link based on WMI query
Preference Targeting

Configuration is defined by policy settings in GPOs. However, the configuration changes in a GPO do not affect computers or users in your enterprise until you have specified the computers or users to which the GPO applies. This is called scoping a GPO. The scope of a GPO is the collection of users and computers that will apply the settings in the GPO.

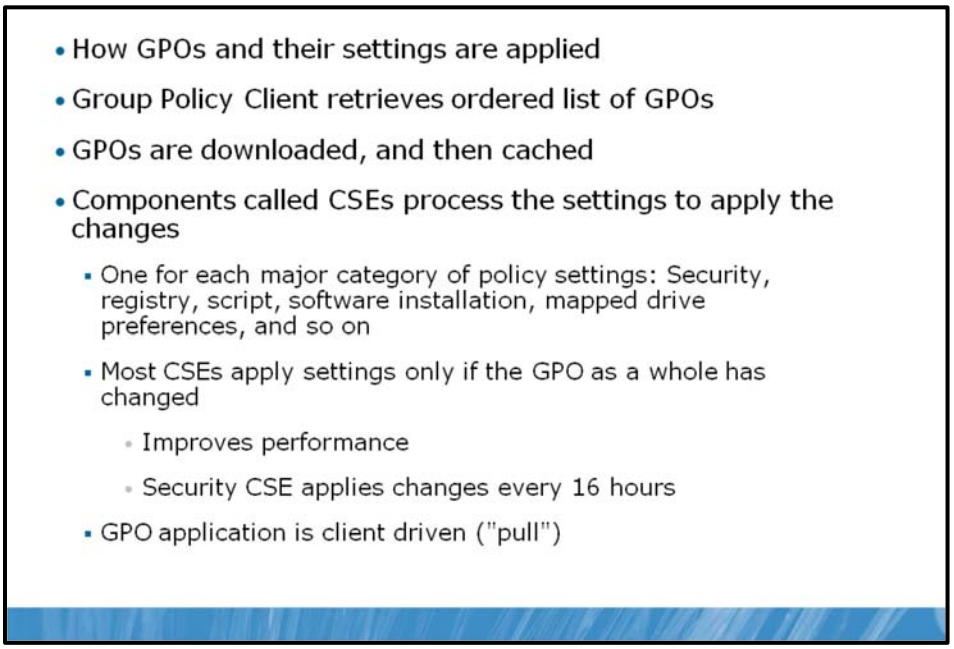
You can use several methods to manage the scope of GPOs. The first is the GPO link. GPOs can be linked to sites, domains, and OUs in Active Directory. The site, domain, or OU then becomes the maximum scope of the GPO. All computers and users within the site, domain, or OU, including those in child OUs, will be affected by the configurations specified by the policy settings in the GPO. A single GPO can be linked to more than one site or OU.

You can further narrow the scope of the GPO with one of two types of filters: security filters that specify global security groups to which the GPO should or should not apply, and Windows Management Instrumentation (WMI) filters that specify a scope by using characteristics of a system, such as operating system version or free disk space. Use security filters and WMI filters to narrow or specify the scope within the initial scope created by the GPO link.

Windows Server® 2008 introduced a new component of Group Policy: Group Policy Preferences. Settings that are configured by Group Policy Preferences within a GPO can be filtered or targeted based on several criteria. Targeted preferences allow you to further refine the scope of Preferences within a single GPO.

MCT USE ONLY. STUDENT USE PROHIBITED

## Group Policy Client and Client-Side Extensions


How GPOs and their settings are applied
Group Policy Client retrieves ordered list of GPOs
GPOs are downloaded, and then cached
Components called CSEs process the settings to apply the changes
One for each major category of policy settings: Security, registry, script, software installation, mapped drive preferences, and so on
Most CSEs apply settings only if the GPO as a whole has changed
Improves performance
Security CSE applies changes every 16 hours
GPO application is client driven ("pull")

How exactly are the policy settings applied? When Group Policy refresh begins, a service running on all Windows systems, which is called the Group Policy Client in Windows Vista®, Windows 7, Windows Server 2008, and Windows Server 2008 R2, determines which GPOs apply to the computer or user. This service downloads any GPOs that are not already cached. Then, a series of processes called client-side extensions (CSEs) interpret the settings in a GPO and make appropriate changes to the local computer or to the currently logged-on user. There are CSEs for each major category of policy setting. For example, there is a security CSE that applies security changes, a CSE that executes startup and logon scripts, a CSE that installs software, and a CSE that makes changes to registry keys and values. Each version of Windows has added CSEs to extend the functional reach of Group Policy. There are several dozen CSEs now in Windows.

One of the more important concepts to remember about Group Policy is that it is really client-driven. The Group Policy client pulls the GPOs from the domain, triggering the CSEs to apply settings locally. Group Policy is not a push technology.

In fact, the behavior of CSEs can be configured by using Group Policy. Most CSEs will apply settings in a GPO only if that GPO has changed. This behavior improves overall policy processing by eliminating redundant applications of the same settings. Most policies are applied in such a way that standard users cannot change the setting on their system—they will always be subject to the configuration enforced by Group Policy. However, some settings can be changed by standard users, and many can be changed if a user is an administrator on that system. If users in your environment are administrators on their computers, consider configuring CSEs to reapply policy settings even if the GPO has not changed. That way, if an administrative user changes a configuration so that it is no longer compliant with policy, the configuration will be reset to its compliant state at the next Group Policy refresh.

MCT USE ONLY. STUDENT USE PROHIBITED

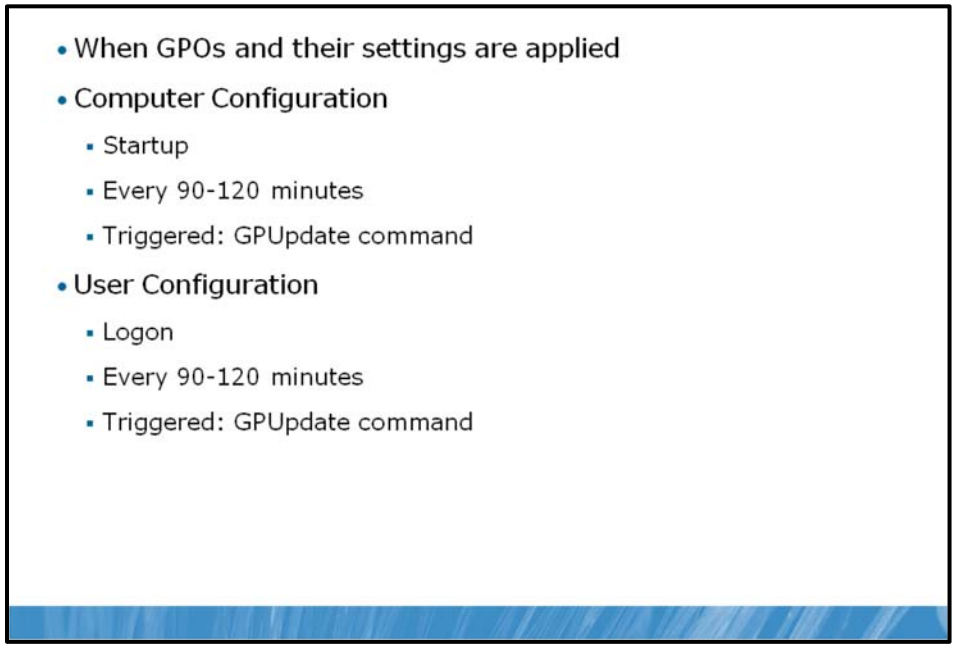
**Note** You can configure CSEs to reapply policy settings, even if the GPO has not changed, at background refresh. To do so, configure a GPO scoped to computers and define the settings in the Computer Configuration\Policies\Administrative Templates\System\ Group Policy node. For each CSE you want to configure, open its policy processing policy setting, such as Registry Policy Processing for the Registry CSE. Click Enabled and select the Process even if the Group Policy objects have not changed check box.

An important exception to the default policy processing settings is settings managed by the security CSE. Security settings are reapplied every 16 hours even if a GPO has not changed.

**Note** Enable the Always Wait For Network At Startup And Logon policy setting for all Windows clients. Without this setting, by default, Windows XP, Windows Vista, and Windows 7 clients perform only background refreshes—a client might start up, and a user might log on without receiving the latest policies from the domain. The setting is located in Computer Configuration\Policies\Administrative Templates\System\Logon. Be sure to read the policy setting's explanatory text. The contoso.com domain used in this course has been preconfigured with this additional Group Policy setting.

MCT USE ONLY. STUDENT USE PROHIBITED

## Group Policy Refresh



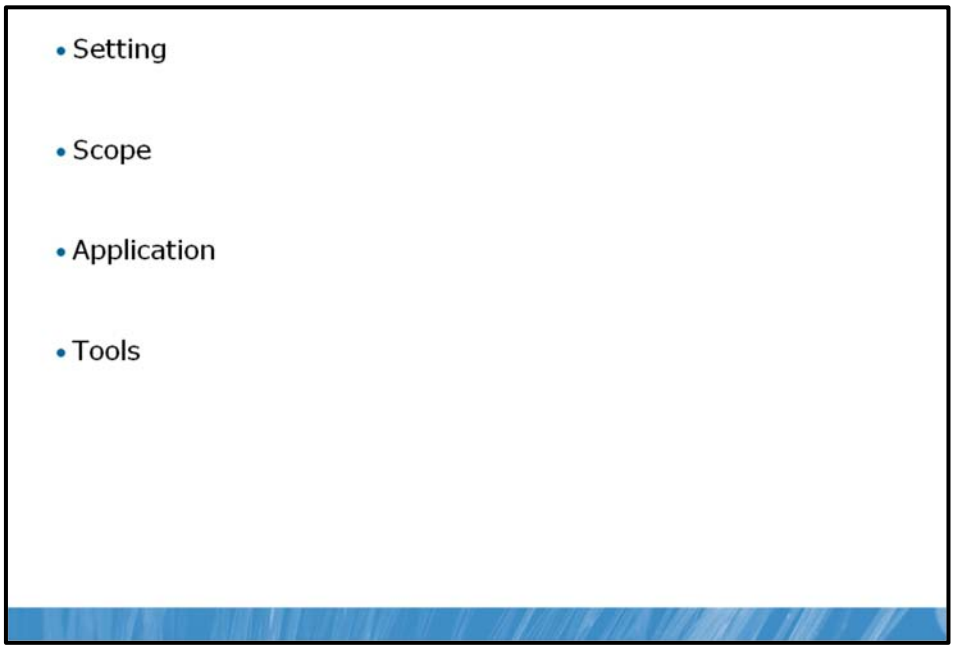

When are policies applied? Policy settings in the Computer Configuration node are applied at system startup and every 90–120 minutes thereafter. User Configuration policy settings are applied at logon and every 90–120 minutes thereafter. The application of policies is called Group Policy refresh.

You can also force a policy refresh by using the **GPUpdate** command.

You will learn more about Group Policy refresh in Lesson 6.

MCT USE ONLY. STUDENT USE PROHIBITED

## Review the Components of Group Policy

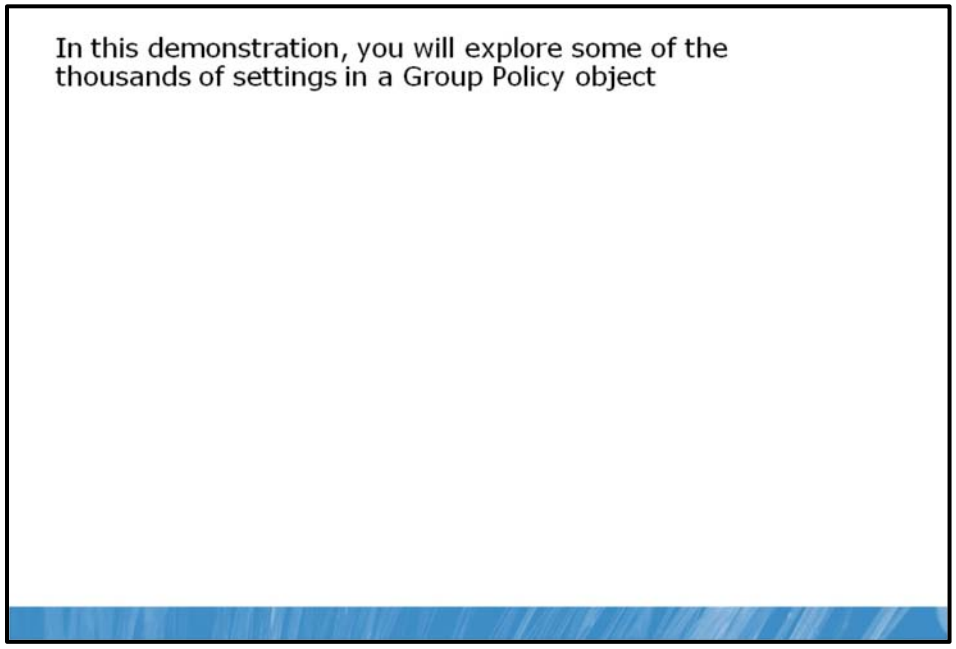



As discussed in previous topics, the most important components to take care of when dealing with Group Policies are:

- Setting. This represents a specific setting that is configurable in each Group Policy object. In Windows Server 2008 R2, there almost 3,000 different settings. Group Policy settings provide the meaning and purpose of Group Policy. Settings can be enabled or disabled, but by default, they are Not Configured. The effect of enabling or disabling a setting can sometimes be complex to evaluate, so be sure to read the explanatory text and test all settings before deploying them in production.
- Scope. After Group Policy settings are configured, you must decide where to apply the GPO. This is defined by scope. A GPO can be linked to a site, domain, or OU. Within the link scope, a GPO can be filtered with security groups or WMI filters.
- Application. When planning Group Policy application, you must be aware of refresh intervals for various types of computers. Computer settings are applied at startup and every 90–120 minutes thereafter. User settings are applied at logon and every 90–120 minutes thereafter.
- Tools. There are several tools for managing GPOs. GPOs are managed through the Group Policy Management console. Policy settings within a GPO are configured by using the GPME. GPUpdate allows you to manually trigger Group Policy refresh. RSoP tools allow you to evaluate and model the settings that were applied by Group Policy.

MCT USE ONLY. STUDENT USE PROHIBITED

## Demonstration: Exploring Group Policy Settings




Group Policy settings, also known as policies, are contained in a GPO and are viewed and modified by using the GPME. In this demonstration, you will look more closely at the categories of settings available in a GPO.

### Computer Configuration and User Configuration

There are two major divisions of policy settings: computer settings, contained in the Computer Configuration node, and user settings, contained in the User Configuration node.

- The Computer Configuration node contains the settings that are applied to computers, regardless of who logs on to them. Computer settings are applied when the operating system starts and during background refresh and every 90–120 minutes thereafter.
- The User Configuration node contains settings that are applied when a user logs on to the computer and during background refresh and every 90–120 minutes thereafter.

Within the Computer Configuration and User Configuration nodes are the Policies and Preferences nodes. Policies are settings that are configured and behave similarly to the policy settings in the earlier versions of Windows. Preferences are introduced in Windows Server 2008. The following sections examine these nodes.

Within the Policies nodes within Computer Configuration and User Configuration are a hierarchy of folders containing policy settings. Because there are thousands of settings, it is beyond the scope of the exam and of this course to examine individual settings. It is worthwhile, however, to define the broad categories of settings in the folders.

### Software Settings Node

The Software Settings node is the first node. It contains only the Software Installation extension. This extension helps you specify how applications are installed and maintained within your organization. It

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

provides a place for independent software vendors to add settings. Software deployment with Group Policy is discussed in Module 7.

### Windows Settings Node

In both Computer Configuration and User Configuration nodes, the Policies node contains a Windows Settings node, which includes the Scripts, Security Settings, and Policy-Based QoS nodes.

The Scripts extension enables you to specify two types of scripts, startup/shutdown (in the Computer Configuration node), and logon/logoff (in the User Configuration node). Startup/shutdown scripts run at computer startup or shutdown. Logon/logoff scripts run when a user logs on or off. When you assign multiple logon/logoff or startup/shutdown scripts to a user or computer, the Scripts CSE executes the scripts from top to bottom. You can determine the order of execution for multiple scripts in the **Properties** dialog box. When a computer is shut down, the CSE first processes logoff scripts, followed by shutdown scripts. By default, the timeout value for processing scripts is 10 minutes. If the logoff and shutdown scripts require more than 10 minutes to process, you must adjust the timeout value with a policy setting. You can use any ActiveX® scripting language to write scripts. Some possibilities include Microsoft Visual Basic® Scripting Edition (VBScript), Microsoft JScript®, Perl, and Microsoft MS-DOS®–style batch files (.bat and .cmd). Logon scripts on a shared network directory in another forest are supported for network logon across forests.

### Security Settings Node

The Security Settings node allows a security administrator to configure security by using GPOs. This can be done after, or instead of, using a security template to set system security. For a detailed discussion of system security and the Security Settings node, refer to Module 7.

### Policy-Based QoS Node

The Policy-Based QoS node defines policies that manage network traffic. For example, you might want to ensure that users in the Finance department have priority for running a critical network application during the end-of-year financial reporting period. The Policy-Based QoS node enables you to do that.

In the User Configuration node only, the Windows Settings folder contains the additional Remote Installation Services, Folder Redirection, and Internet Explorer Maintenance nodes. Remote Installation Services (RIS) policies control the behavior of a remote operating system installation. Folder Redirection enables you to redirect user data and settings folders such as AppData, Desktop, Documents, Pictures, Music, and Favorites from their default user profile location to an alternate location on the network, where they can be centrally managed. Internet Explorer Maintenance enables you to administer and customize Microsoft Internet Explorer®.

### Administrative Templates Node

In the Computer Configuration and User Configuration nodes, the Administrative Templates node contains registry-based Group Policy settings. The Administrative Templates node is discussed in detail later in this module.

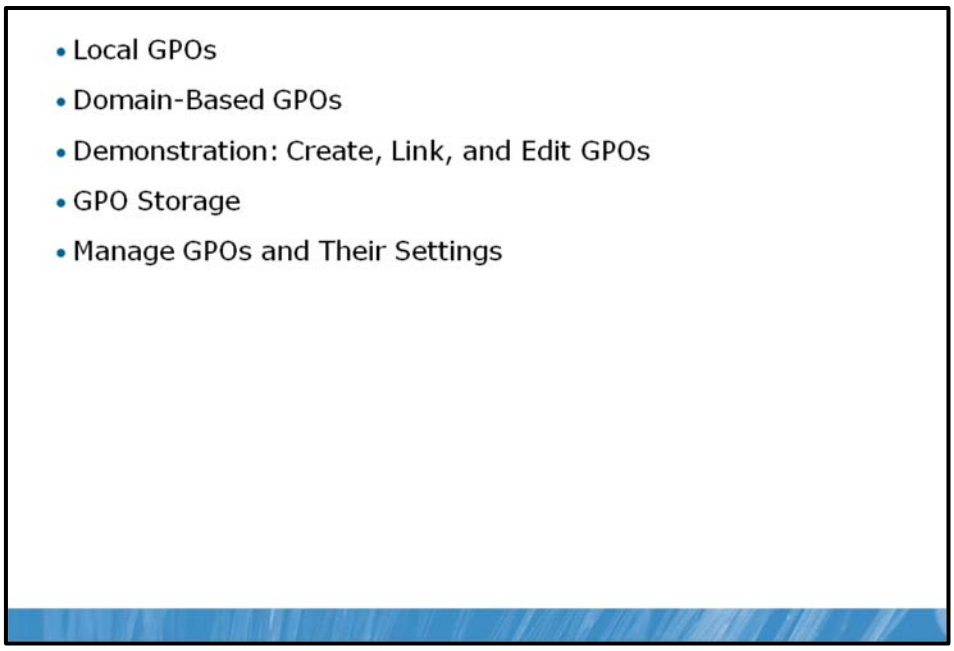
There are thousands of such settings available for configuring the user and computer environment. As an administrator, you might spend a significant amount of time manipulating these settings. To assist you with the settings, a description of each policy setting is available in two locations:

- On the **Explain** tab in the **Properties** dialog box for the setting. In addition, the **Settings** tab in the **Properties** dialog box for each setting also lists the required operating system or software for the setting.

- On the **Extended** tab of the GPME. The **Extended** tab appears on the lower right of the details pane and provides a description of each selected setting in a column between the console tree and the settings pane. The required operating system or software for each setting is also listed.

MCT USE ONLY. STUDENT USE PROHIBITED

# Lesson 2
# Implement GPOs




Now that you have a broad understanding of Group Policy and its components, you can look closely at each component. In this section, you will examine GPOs in detail.

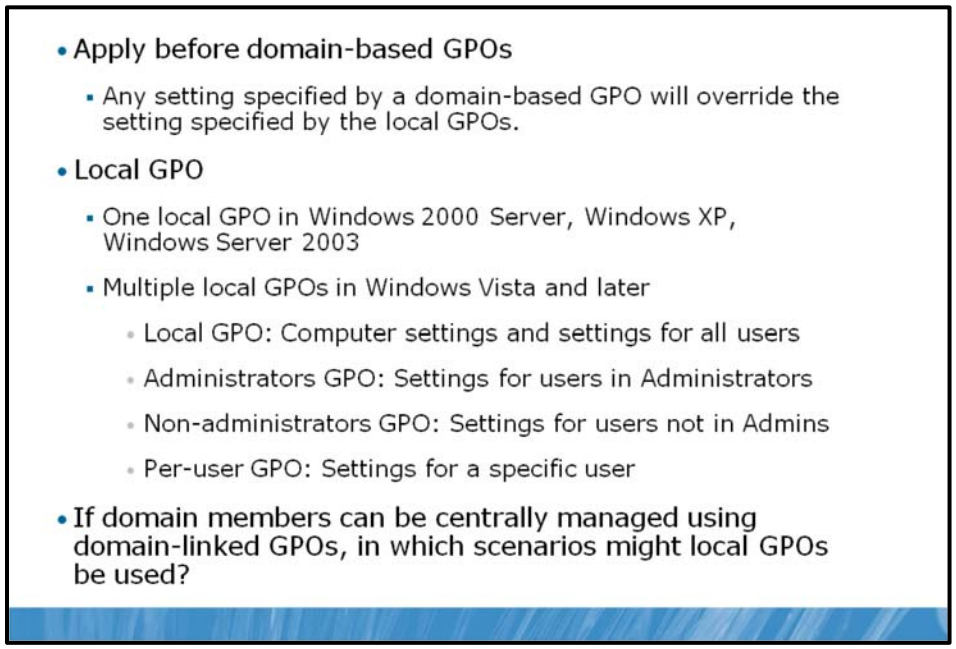
### Objectives

After completing this lesson, you will be able to:

- Create, edit, and link GPOs.
- Identify change and configuration management capabilities of Group Policy.
- Configure policy settings.
- Explain GPO storage, replication, and versioning.

MCT USE ONLY. STUDENT USE PROHIBITED

## Local GPOs


• Apply before domain-based GPOs
▪ Any setting specified by a domain-based GPO will override the setting specified by the local GPOs.
• Local GPO
▪ One local GPO in Windows 2000 Server, Windows XP, Windows Server 2003
▪ Multiple local GPOs in Windows Vista and later
◦ Local GPO: Computer settings and settings for all users
◦ Administrators GPO: Settings for users in Administrators
◦ Non-administrators GPO: Settings for users not in Admins
◦ Per-user GPO: Settings for a specific user
• If domain members can be centrally managed using domain-linked GPOs, in which scenarios might local GPOs be used?

To manage configuration for users and computers, you create GPOs that contain the policy settings you require. Each computer has several GPOs stored locally on the system, known as the local GPOs, and can be within the scope of any number of domain-based GPOs.

Computers that run Windows 2000 Server, Windows XP, and Windows Server 2003 have one local GPO each, which can manage that system's configuration. The local GPO exists whether or not the computer is part of a domain, a workgroup, or a non-networked environment. It is stored in %SystemRoot%\System3\GroupPolicy. The policies in the local GPO affect only the computer on which the GPO is stored. By default, only the Security Settings policies are configured on a system's local GPO. All other policies are set at Not Configured.

When a computer does not belong to an Active Directory domain, the local policy is useful to configure and enforce configuration on that computer. However, in an Active Directory domain, settings in GPOs that are linked to the site, domain, or OUs will override local GPO settings and are easier to manage than GPOs on individual computers.

Windows Vista, Windows 7, Windows Server 2008, and later systems have multiple local GPOs. The Local Computer GPO is the same as the GPO in the previous versions of Windows. In the Computer Configuration node, you can configure all computer-related settings. In the User Configuration node, you can configure settings you want to apply to all users on the computer. The user settings in the Local Computer GPO can be modified by the user settings in two new local GPOs: Administrators and Non-Administrators. These two GPOs apply user settings to logged-on users according to whether they are members of the local Administrators group in which case they would use the Administrators GPO or not members of the Administrators group (and use the Non-Administrators GPO). You can further refine the user settings with a local GPO that applies to a specific user account. User-specific local GPOs are associated with local, not domain, user accounts.

RSoP is easy for computer settings: The Local Computer GPO is the only local GPO that can apply computer settings. User settings in a user-specific GPO override conflicting settings in the Administrators

MCT USE ONLY. STUDENT USE PROHIBITED

and Non-Administrators GPOs, which themselves override settings in the Local Computer GPO. The concept is simple—the more specific the local GPO, the higher the precedence of its settings.

To create and edit local GPOs:

1. Click the **Start** button and in the **Start Search** box, type **mmc.exe,** and then press Enter.

   An empty Microsoft® Management console (MMC) opens.

2. Click **File,** and then click **Add/Remove Snap-in**.

3. Select the **Group Policy Object Editor option,** and then click **Add**.

   A dialog box appears, prompting you to select the GPO to edit.

4. The **Local Computer GPO** is selected by default. If you want to edit another local GPO, click the **Browse** button. On the **Users** tab, you will find the **Non-Administrators** and **Administrators** GPOs and one GPO for each local user. Select the GPO and click **OK**.

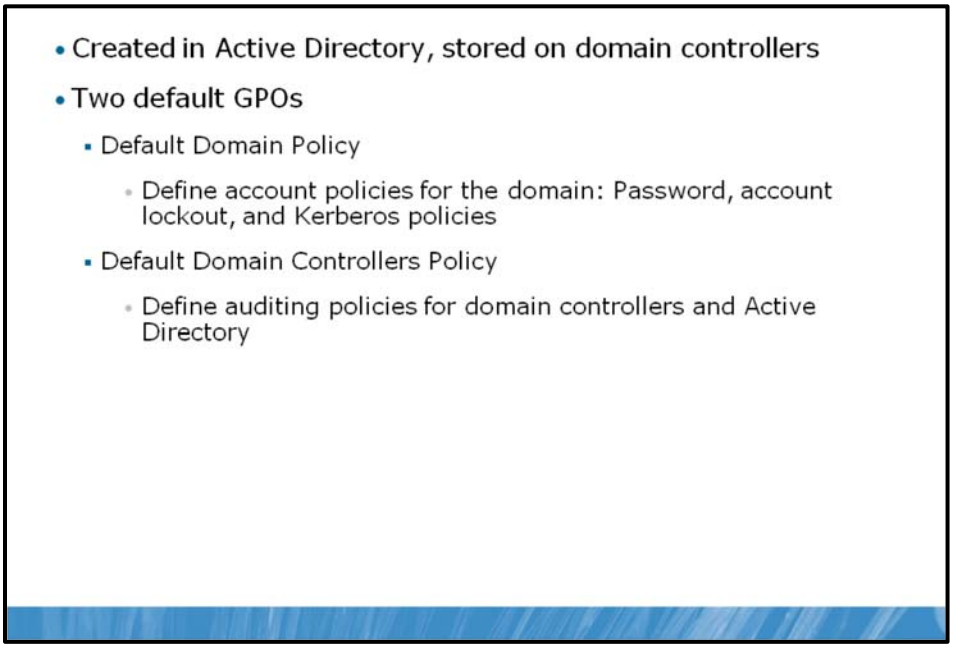
5. Click **Finish,** and then click **OK** to close each of the dialog boxes.

The Group Policy Object Editor snap-in is added and focused on the selected GPO.

**Question:** If domain members can be centrally managed by using domain-linked GPOs, in which scenarios can you use local GPOs?

MCT USE ONLY. STUDENT USE PROHIBITED

## Domain-Based GPOs


• Created in Active Directory, stored on domain controllers
• Two default GPOs
▪ Default Domain Policy
◦ Define account policies for the domain: Password, account lockout, and Kerberos policies
▪ Default Domain Controllers Policy
◦ Define auditing policies for domain controllers and Active Directory

Domain-based GPOs are created in Active Directory and stored on domain controllers. They are used to manage configuration centrally for users and computers in the domain. The remainder of this course refers to domain-based GPOs rather than local GPOs, unless otherwise specified.

When AD DS is installed, two default GPOs are created: Default Domain Controllers Policy and Default Domain Policy.

### Default Domain Policy

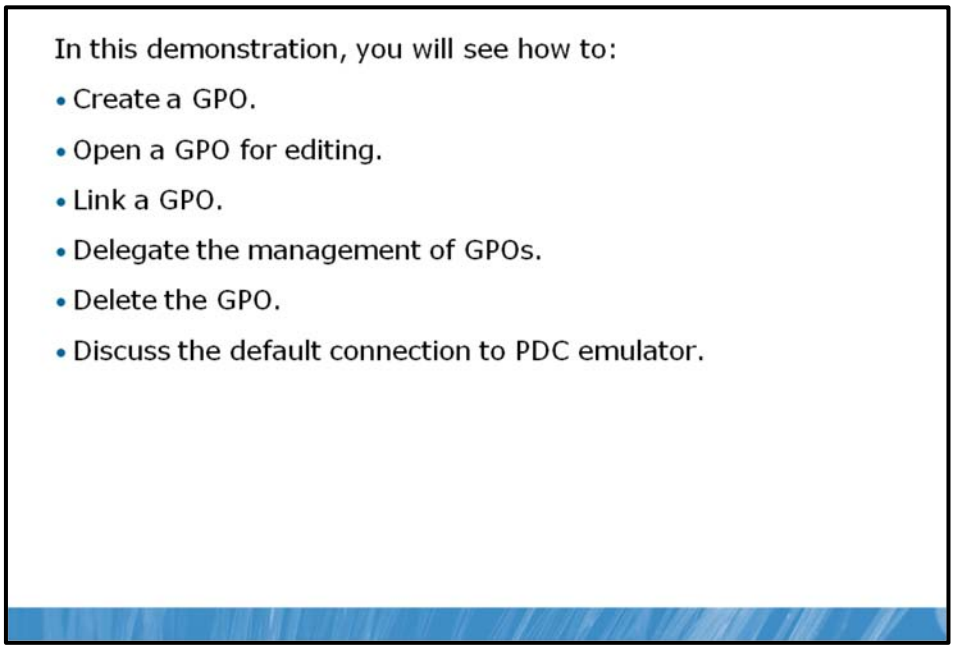
This GPO is linked to the domain and has no security group or WMI filters. Therefore, it affects all users and computers in the domain, including computers that are domain controllers. This GPO contains policy settings that specify password, account lockout, and Kerberos policies. In Module 10, you will learn how to modify the default settings in this GPO to align with your enterprise password and account lockout policies. You should not add unrelated policy settings to this GPO. If you need to configure other settings to apply broadly in your domain, create additional GPOs linked to the domain.

### Default Domain Controllers Policy

This GPO is linked to the OU of the domain controllers. Because computer accounts for domain controllers are kept exclusively in the Domain Controllers OU, and other computer accounts should be kept in other OUs, this GPO affects only domain controllers. The Default Domain Controllers GPO should be modified to implement your auditing policies, as you will see in Modules 8 through 10. It should also be modified to assign user rights required on domain controllers.

MCT USE ONLY. STUDENT USE PROHIBITED

## Demonstration: Create, Link, and Edit GPOs


In this demonstration, you will see how to:
• Create a GPO.
• Open a GPO for editing.
• Link a GPO.
• Delegate the management of GPOs.
• Delete the GPO.
• Discuss the default connection to PDC emulator.

To create a GPO, right-click the **Group Policy Objects** container, and then click **New**.

You must have permission to the Group Policy Objects container to create a GPO. By default, the Domain Admins group and the Group Policy Creator Owners group are delegated the ability to create GPOs.

To delegate permission to create GPOs to other groups, select the Group Policy Objects container in the GPMC console tree and then click the **Delegation** tab in the console details pane.

After you have created a GPO, you can create the initial scope of the GPO by linking it to a site, domain, or OU.

To link a GPO, right-click the site, domain, or OU, and then click **Link An Existing GPO**.

You can also create and link a GPO with a single step: right-click a site, domain, or OU, and then click **Create A GPO In This Domain And Link It Here**.

Note that you will not see your sites in the Sites node of the GPMC until you right-click **Sites**, click **Show Sites**, and then select the sites you want to manage.

You must have permission to link GPOs to a site, domain, or OU. In the GPMC, select the container in the console tree, and then click the **Delegation** tab in the console details pane. From the **Permission** drop-down list, click **Link GPOs**. The users and groups displayed hold the permission for the selected OU. Click the **Add** or **Remove** buttons to modify the delegation.

To edit a GPO, right-click the GPO in the Group Policy Objects container and click **Edit**.

The GPO is opened in the GPME. You must have at least the Read permission to open the GPO in this way.

To make changes to a GPO, you must have the Write permission to the GPO. Permissions for the GPO can be set by selecting the GPO in the Group Policy Objects container and then clicking the **Delegation** tab in the details pane.

MCT USE ONLY. STUDENT USE PROHIBITED

The GPME will display the name of the GPO as the root node. The GPME also displays the domain in which the GPO is defined and the server from which the GPO was opened and to which changes will be saved. The root node is in the GPO Name [Server Name] format. In the screenshot of the GPME on an earlier page in this module, the root node is CONTOSO Standards [SERVER01.contoso.com] Policy. The GPO name is CONTOSO Standards, and it was opened from SERVER01.contoso.com, meaning that the GPO is defined in the contoso.com domain.

By default, both the GPMC and the GPME console connect to a specific domain controller in your environment with the domain controller acting as the PDC Emulator. In a later module, you will learn to identify and manage which domain controller has this role.

This is done to reduce the possibility that a single GPO might be changed on two different domain controllers, at which point during replication there would be no way to reconcile the changes, and only one version of the entire GPO would prevail and be replicated. Focusing the administrative tools on one domain controller helps ensure that changes are made in one place.

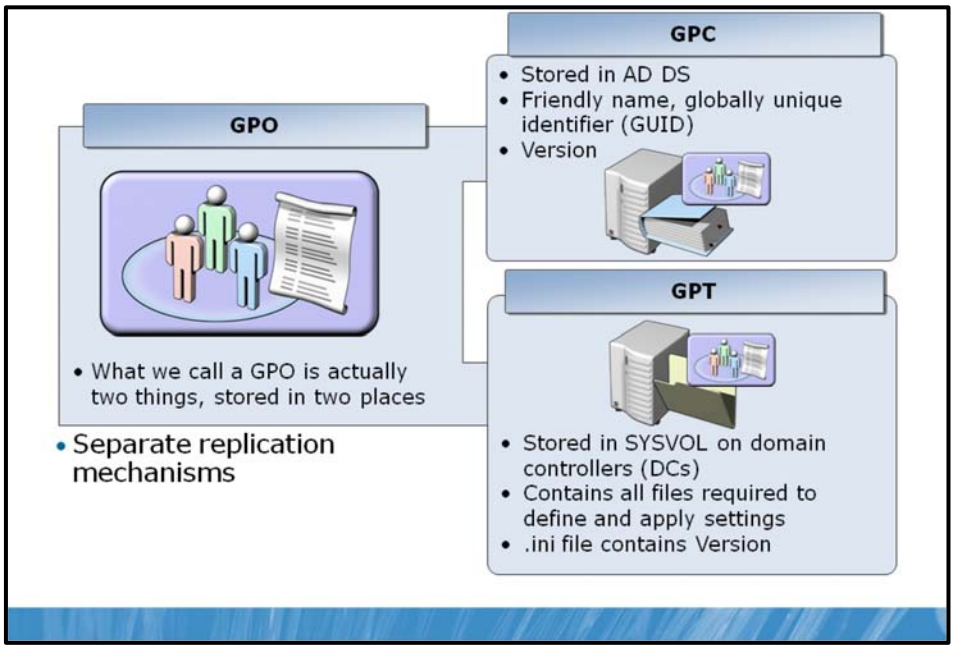
However, in a large, distributed environment, the PDC Emulator may be in a distant site, resulting in slow performance for the GPMCs. You can right-click the root node of each console and connect to a specific domain controller closer to you. Just be cognizant of the replication issue: If you are the only one who is editing a GPO, it is perfectly acceptable for you to do so on a local, higher performing domain controller.

### Demonstration Steps

- Create a GPO.
- Open a GPO for editing.
- Link a GPO.
- Delegate the management of GPOs.
- Delete the GPO.
- Discuss the default connection to PDC emulator.

MCT USE ONLY. STUDENT USE PROHIBITED

## GPO Storage


GPC
• Stored in AD DS
• Friendly name, globally unique identifier (GUID)
• Version
GPO
• What we call a GPO is actually two things, stored in two places
• Separate replication mechanisms
GPT
• Stored in SYSVOL on domain controllers (DCs)
• Contains all files required to define and apply settings
• .ini file contains Version

Group Policy settings are presented as GPOs in Active Directory user interface tools, but a GPO is actually two components: a Group Policy Container (GPC)and a Group Policy Template (GPT).

The GPC is an Active Directory object stored in the Group Policy Objects container within the domain-naming context of the directory. Like all Active Directory objects, each GPC includes a globally unique identifier (GUID) attribute that uniquely identifies the object within Active Directory. The GPC defines basic attributes of the GPO, but it does not contain any of the settings. The settings are contained in the GPT; a collection of files stored in the SYSVOL of each domain controller in the %SystemRoot%\SYSVOL\Domain\Policies\GPOGUID path, where GPOGUID is the GUID of the GPC. When you make changes to the settings of a GPO, the changes are saved to the GPT of the server from which the GPO was opened.

By default, when Group Policy refresh occurs, the CSEs apply settings in a GPO only if the GPO has been updated.

The Group Policy client can identify an updated GPO by its version number. Each GPO has a version number that is incremented each time a change is made. The version number is stored as an attribute of the GPC and in a text file, GPT.ini, in the GPT folder. The Group Policy client knows the version number of each GPO it has previously applied. If, during Group Policy refresh, the Group Policy client discovers that the version number of the GPC has been changed, the CSEs will be informed that the GPO is updated.

### GPO Replication

Group Policy Container and Group Policy Template are both replicated between all domain controllers in Active Directory. However, different replication mechanisms are used for these two items.

The GPC in Active Directory is replicated by the Directory Replication Agent (DRA). The DRA uses a topology generated by the Knowledge Consistency Checker (KCC) that can be defined or refined manually. You will learn more about Active Directory Replication in Module 14. The result is that the GPC

MCT USE ONLY. STUDENT USE PROHIBITED

is replicated within seconds to all domain controllers in a site and is replicated between sites based on your intersite replication configuration. This process will also be discussed in Module 14.

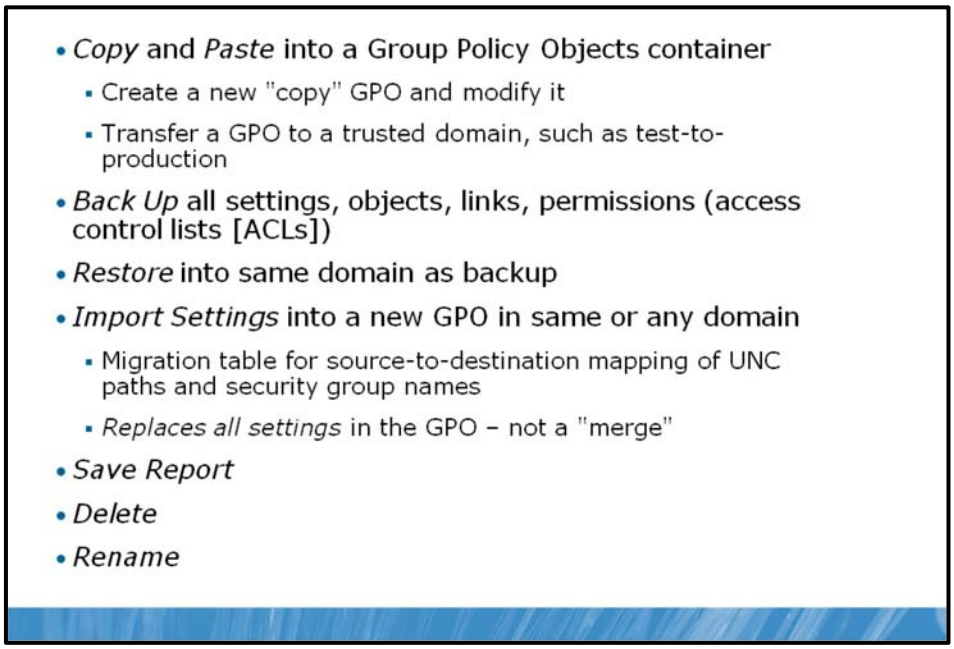
The GPT in the SYSVOL is replicated by using one of the following two technologies. The File Replication Service (FRS) is used to replicate SYSVOL in domains running Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, and Windows 2000. If all domain controllers are running Windows Server 2008 or earlier, you can configure SYSVOL replication by using Distributed File System Replication (DFSR), which is a much more efficient and robust mechanism.

Because the GPC and GPT are replicated separately, it is possible for them to become out of sync for a short time.

Typically, when this happens, the GPC will replicate to a domain controller first. Systems that obtained their ordered list of GPOs from that domain controller will identify the new GPC, will attempt to download the GPT, and will notice that the version numbers are not the same. A policy processing error will be recorded in the event logs. If the reverse happens, and the GPO replicates to a domain controller before the GPC, clients obtaining their ordered list of GPOs from that domain controller will not be notified of the new GPO until the GPC has replicated.

MCT USE ONLY. STUDENT USE PROHIBITED

## Manage GPOs and Their Settings

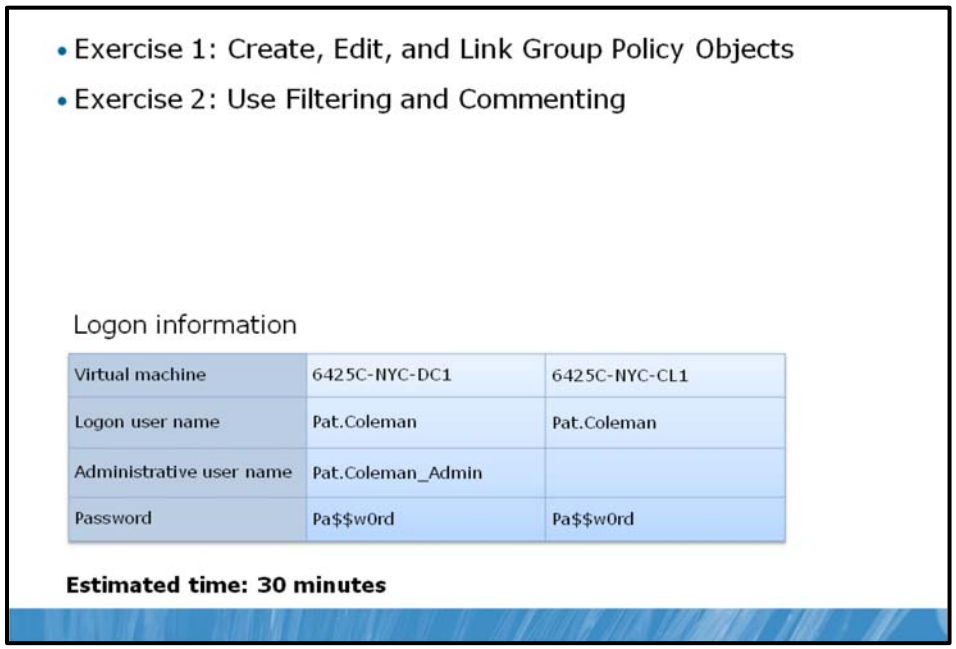

• *Copy* and *Paste* into a Group Policy Objects container
▪ Create a new "copy" GPO and modify it
▪ Transfer a GPO to a trusted domain, such as test-to-production
• *Back Up* all settings, objects, links, permissions (access control lists [ACLs])
• *Restore* into same domain as backup
• *Import Settings* into a new GPO in same or any domain
▪ Migration table for source-to-destination mapping of UNC paths and security group names
▪ *Replaces all settings* in the GPO – not a "merge"
• *Save Report*
• *Delete*
• *Rename*

When you right-click a GPO in the GPMC, a list of useful management commands appears.

- **Copy.** You can copy a GPO and then right-click the Group Policy Objects container and select Paste to create a copy of the GPO. This is useful when you want to create a new GPO in the same domain and to start with the same settings as an existing GPO. It is also useful to copy a GPO into another domain, for example, between a test domain and a production domain. To copy a GPO between domains, add the target trusted domain to the GPMC. You must have permission to create GPOs in the target domain. When you paste a GPO, you are given the option to copy the access control list (ACL) from the original GPO, which preserves the security filtering, or to use the default ACL for new GPOs in the target domain.
- **Back Up.** As with any critical data, it is important to back up GPOs. Because a GPO consists of several files, objects, permissions, and links, managing the backup and restore of GPOs is quite difficult. Luckily, the **Back Up** command pulls all of those pieces into a single place and makes restore a simple task.
- **Restore from Backup.** Restore an entire GPO, including its files, objects, permissions, and links into the same domain in which the GPO originally existed.
- **Import Settings.** Import only the settings from a backed-up GPO. Although this option does not import permissions or links, it can be useful for transferring GPOs between nontrusted domains that cannot use copy and paste. If a GPO includes potentially domain-specific settings, including the UNC paths or names of security groups, you will be prompted as to whether you want to import those settings exactly as they were backed up or to use a migration table that maps source to destination names.
- **Save Report.** Use this to save an HTML report of the GPO settings.
- **Delete.** Use this to delete a GPO.
- **Rename.** Use this to rename a GPO.

MCT USE ONLY. STUDENT USE PROHIBITED

# Lab A: Implement Group Policy


• Exercise 1: Create, Edit, and Link Group Policy Objects
• Exercise 2: Use Filtering and Commenting
Logon information
Virtual machine | 6425C-NYC-DC1 | 6425C-NYC-CL1
Logon user name | Pat.Coleman | Pat.Coleman
Administrative user name | Pat.Coleman_Admin |
Password | Pa$$w0rd | Pa$$w0rd
Estimated time: 30 minutes

## Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V™ Manager, click **6425C-NYC-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
   - User name: **Pat.Coleman**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
5. Start 6425C-NYC-CL1. Do not log on to the client computer until directed to do so.

## Lab Scenario

You are responsible for managing change and configuration at Contoso, Ltd. Contoso corporate IT security policies specify that computers cannot be left unattended and logged on to for more than 10 minutes. You will therefore configure the screen-saver timeout and password-protected screen-saver policy settings. Additionally, you will lock down access to registry editing tools.

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 1: Create, Edit, and Link Group Policy Objects

In this exercise, you will create a GPO that implements a setting mandated by the corporate security policy of Contoso, Ltd and scope the setting to all users and computers in the domain. You will then examine the effect of the GPO. You can also explore other settings that are made available within a GPO.

The main tasks for this exercise are as follows:

1. Create a GPO.
2. Edit the settings of a GPO.
3. Scope a GPO with a GPO link.
4. View the effects of Group Policy application.
5. Explore GPO settings.

### ▶ Task 1: Create a GPO.

1. On NYC-DC1, run **Group Policy Management** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd.**
2. Create a **Group Policy Object** named **CONTOSO Standards** in the **Group Policy Objects** container.

### ▶ Task 2: Edit the settings of a GPO.

1. Edit the **CONTOSO Standards** GPO.
2. Navigate to the **User Configuration, Policies, Administrative Templates, System** folder.
3. Prevent users from running **Registry Editor** and **regedit /s**.
4. Navigate to the **User Configuration, Policies, Administrative Templates, Control Panel, Personalization** folder.
5. Examine the explanatory text for the **Screen saver timeout** policy setting.
6. Configure the **Screen saver timeout** policy to **600** seconds.
7. Enable the **Password protect the screen saver** policy setting.

### ▶ Task 3: Scope a GPO with a GPO link.

- Link the **CONTOSO Standards** GPO to the **contoso.com** domain.

### ▶ Task 4: View the effects of Group Policy application.

1. Log on to NYC-CL1 as **Pat.Coleman**.
2. Attempt to change the screen saver wait time and resume settings. You are prevented from doing so by Group Policy.
3. Attempt to run **Registry Editor**. You are prevented from doing so by Group Policy.

MCT USE ONLY. STUDENT USE PROHIBITED

▶ Task 5: Explore GPO settings.

- On NYC-DC1, edit the **CONTOSO Standards** GPO and spend time exploring the settings that are available in a GPO. Do not make any changes.

**Results:** In this exercise, you created a GPO named Contoso Standards that configures password-protected screen saver, screen-saver timeout, and registry editing tool restrictions

**Note** Do not shut down the virtual machines after you finish this lab because the settings you have configured here will be used in subsequent labs.

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 2: Use Filtering and Commenting

In this exercise, you will use the new commenting and filtering features of Group Policy to locate and document policy settings.

The main tasks for this exercise are as follows:

1. Search and filter policy settings.
2. Document GPOs and settings with comments.

### ▶ Task 1: Search and filter policy settings.

1. If necessary, open the GPMC and then edit the **CONTOSO Standards** GPO.
2. In the **User Configuration\Policies\Administrative Templates** folder, filter the view to show only policy settings that contain the phrase **screen saver**. Spend a few moments examining those settings.
3. Filter the view to show only configured policy settings. Spend a few moments examining those settings.
4. Turn off the filter from **Administrative Templates**.

### ▶ Task 2: Document GPOs and settings with comments.

1. Edit the comment to the **CONTOSO Standards** GPO and add the following comment to the GPO: **Contoso corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO:** *your name*.

   This comment appears on the **Details** tab of the GPO in the GPMC.
2. Add the following comment to the **Screen saver timeout** policy setting: **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver**.
3. Add the following comment to the **Password protect the screen saver** policy setting: **Corporate IT Security Policy implemented with this policy in combination with Screen Saver Timeout**.

**Results:** In this exercise, you added comments to your Group Policy object and settings.

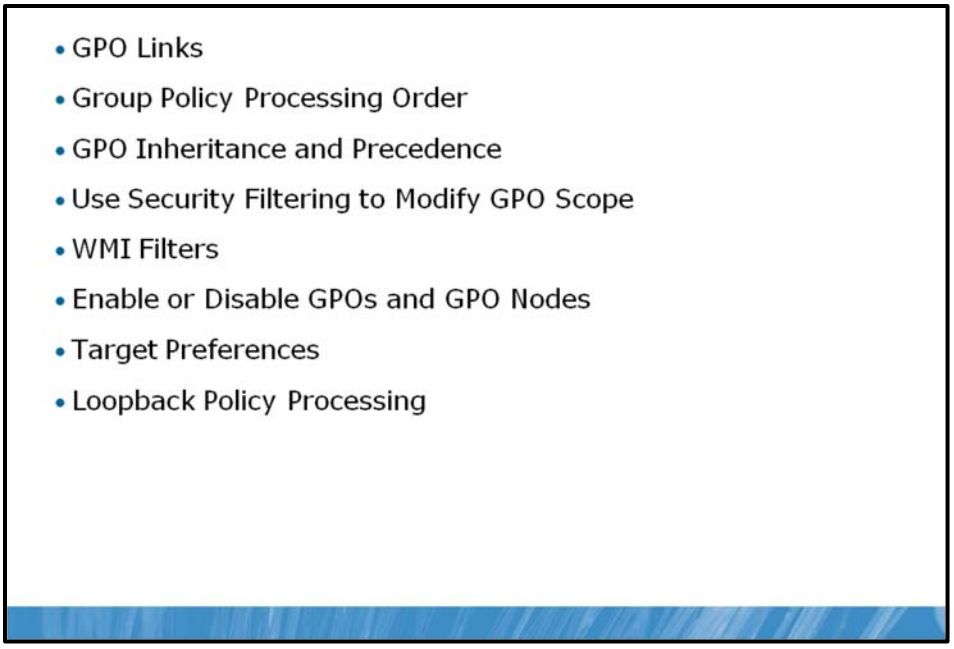
### Lab Review Questions

**Question:** Which policy settings are already being deployed by using Group Policy in your organization?

**Question:** Which policy settings did you discover that you might want to implement in your organization?

MCT USE ONLY. STUDENT USE PROHIBITED

# Lesson 3
# Manage Group Policy Scope


• GPO Links
• Group Policy Processing Order
• GPO Inheritance and Precedence
• Use Security Filtering to Modify GPO Scope
• WMI Filters
• Enable or Disable GPOs and GPO Nodes
• Target Preferences
• Loopback Policy Processing

A GPO is, by itself, a collection of configuration instructions that will be processed by the CSEs of computers. Until the GPO is scoped, it does not apply to any users or computers. The GPO's scope determines the CSEs of which computers will receive and process the GPO and only the computers or users within the scope of a GPO will apply the settings in that GPO. In this lesson, you will learn to manage the scope of a GPO. The following mechanisms are used to scope a GPO:

- The GPO link to a site, domain, or OU and whether that link is enabled
- The Enforce option of a GPO
- The Block Inheritance option on an OU
- Security group filtering
- WMI filtering
- Policy node enabling or disabling
- Preferences targeting
- Loopback policy processing

You must be able to define the users or computers to which configuration is deployed, and therefore, you must master the art of scoping GPOs. In this lesson, you will learn each of the mechanisms with which you can scope a GPO and, in the process, you will master the concepts of Group Policy application, inheritance, and precedence.

### Objectives

After completing this lesson, you will be able to:

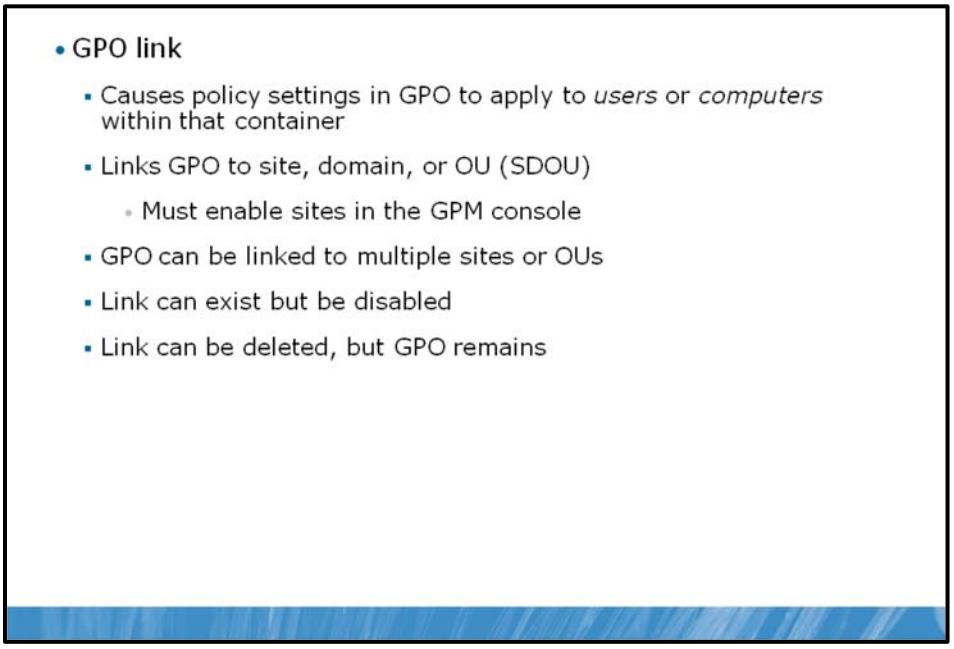
- Manage GPO links.

MCT USE ONLY. STUDENT USE PROHIBITED

- Identify the relationship between OU structure and GPO application.
- Evaluate GPO inheritance and precedence.
- Understand the Block Inheritance and Enforced link options.
- Apply security filtering to narrow the scope of a GPO.
- Apply a WMI filter to a GPO.
- Target Group Policy preferences.
- Identify best practices for scoping Group Policy.

MCT USE ONLY. STUDENT USE PROHIBITED

## GPO Links


GPO link
Causes policy settings in GPO to apply to users or computers within that container
Links GPO to site, domain, or OU (SDOU)
Must enable sites in the GPM console
GPO can be linked to multiple sites or OUs
Link can exist but be disabled
Link can be deleted, but GPO remains

A GPO can be linked to one or more Active Directory sites, domains, or OUs. After a policy is linked to a site, domain, or OU, the users or computers and users in that container are within the scope of the GPO, including computers and users in child OUs.

As you learned in Lesson 1, you can link a GPO to the domain, site or to an OU.

To link a GPO, right-click the domain or OU in the GPMC console tree, and then click **Link as existing GPO**. If you have not yet created a GPO, click **Create A GPO In This {Domain | OU | Site} And Link It Here**.

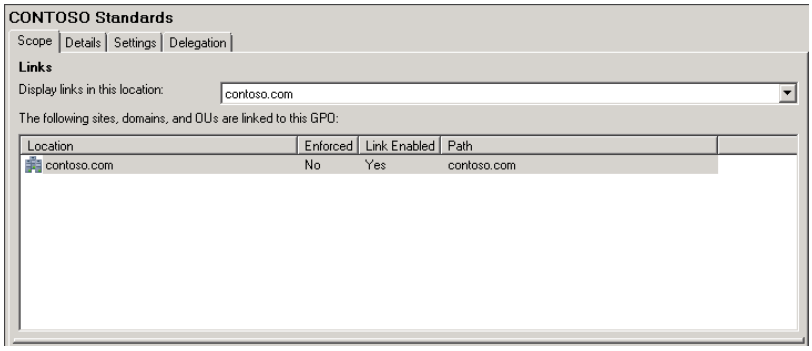
You can choose the same commands to link a GPO to a site, but by default, your Active Directory sites are not visible in the GPMC.

To show sites in the GPMC, right-click Sites in the GPMC console tree and choose **Show Sites**.

**Note** A GPO linked to a site affects all computers in the site without regard to the domain to which the computers belong (as long as all computers belong to the same Active Directory forest). Therefore, when you link a GPO to a site, that GPO can be applied to multiple domains within a forest. Site-linked GPOs are stored on domain controllers in the domain in which the GPO was created. Therefore, domain controllers for that domain must be accessible for site-linked GPOs to be applied correctly. If you implement site-linked policies, you must consider policy application when planning your network infrastructure. Either place a domain controller from the GPO's domain in the site to which the policy is linked, or ensure that a wide area network (WAN) connectivity provides accessibility to a domain controller in the GPO's domain.

MCT USE ONLY. STUDENT USE PROHIBITED

When you link a GPO to a site, domain, or OU, you define the initial scope of the GPO. Select a GPO and click the Scope tab to identify the containers to which the GPO is linked. In the details pane of the GPMC, the GPO links are displayed in the first section of the Scope tab, as seen here:



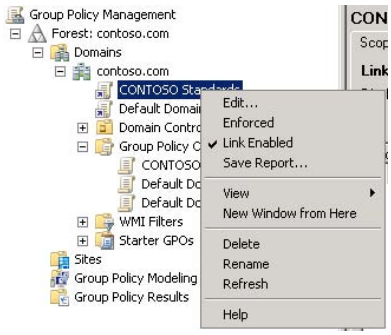

The impact of the GPO's links is that the Group Policy Client downloads the GPO if either the computer or the user objects fall within the scope of the link. The GPO will be downloaded only if it is new or updated. The Group Policy Client caches the GPO to make policy refresh more efficient.

## Link a GPO to Multiple OUs

You can link a GPO to more than one site or OU. It is common, for example, to apply configuration to computers in several OUs. You can define the configuration in a single GPO and link that GPO to each OU. If you later change settings in the GPO, your changes will apply to all OUs to which the GPO is linked.

## Delete or Disable a GPO Link

After you have linked a GPO, the GPO link appears in the GPMC underneath the site, domain, or OU. The icon for the GPO link has a small shortcut arrow. When you right-click the GPO link, a context menu appears, as shown here:




To delete a GPO link, right-click the GPO link in the GPMC console tree and then click **Delete**.

Deleting a GPO link does not delete the GPO itself, which remains in that GPO container. Deleting the link does change the scope of the GPO so that it no longer applies to computers and users within a site, domain, or OU to which it was previously linked.

You can also modify a GPO link by disabling it.

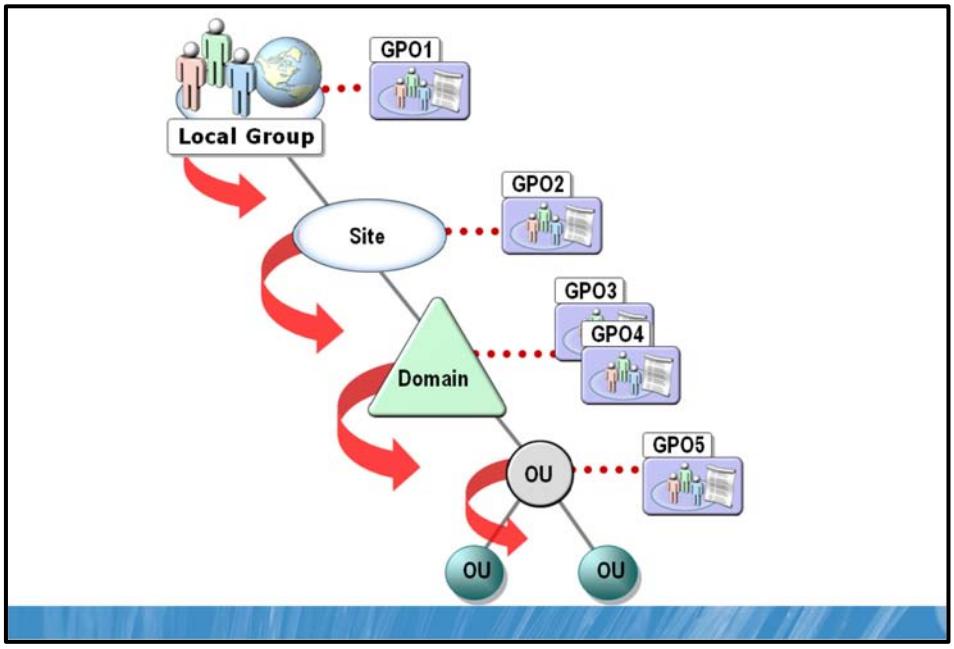
To disable a GPO link, right-click the GPO link in the GPMC console tree and then deselect the **Link Enabled** option.

MCT USE ONLY. STUDENT USE PROHIBITED

Disabling the link also changes the GPO scope so that it no longer applies to computers and users within that container. However, the link remains so that it can be easily re-enabled.

MCT USE ONLY. STUDENT USE PROHIBITED

## Group Policy Processing Order




The GPOs that apply to a user, computer, or both do not all apply at once. GPOs are applied in a particular order. This order means that settings that are processed first may be overwritten by conflicting settings that are processed later.

Group Policy follows the following hierarchical processing order:

1. **Local group policies**. Each computer running Windows 2000 or later has at least one local group policy. The local policies are applied first.
2. **Site group policies**. Policies linked to sites are processed second. If there are multiple site policies, they are processed synchronously in the listed preference order.
3. **Domain group policies**. Policies linked to domains are processed third. If there are multiple domain policies, they are processed synchronously in the listed preference order.
4. **OU group policies**. Policies linked to top-level OUs are processed fourth. If there are multiple top-level OU policies, they are processed synchronously in the listed preference order.
5. **Child OU group policies**. Policies linked to child OUs are processed fifth. If there are multiple child OU policies, they are processed synchronously in the listed preference order. When there are multiple levels of child OUs, policies for higher-level OUs are applied first and policies for the lower-level OUs are applied next.

In Group Policy application, the general rule is that the last policy applied wins. For example, a policy that restricts access to Control Panel applied at the domain level could be reversed by a policy applied at the OU level for the objects contained in that particular OU.

If you link several GPOs to an organizational unit, their processing occurs in the order that the administrator specifies on the Linked Group Policy Objects tab for the organizational unit in the Group Policy Management Console (GPMC).

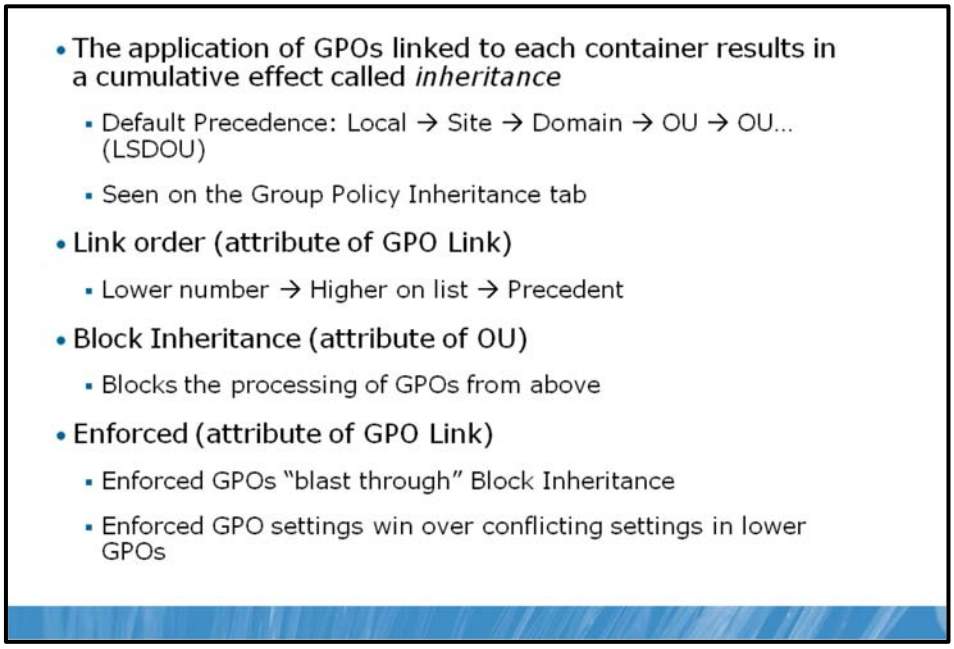
MCT USE ONLY. STUDENT USE PROHIBITED

By default, processing is enabled for all GPO links. You can completely block the application of a GPO for a given site, domain, or organizational unit by disabling that container's GPO link. Note that if the GPO is linked to other containers, they will continue to process the GPO if their links are enabled.

You can also disable the user or computer configuration of a particular GPO independent of either the user or computer. If one section of a policy is known to be empty, disabling the other side speeds up policy processing. For example, if you have a policy that only delivers user desktop configuration, you could disable the computer side of the policy.

MCT USE ONLY. STUDENT USE PROHIBITED

## GPO Inheritance and Precedence


• The application of GPOs linked to each container results in a cumulative effect called *inheritance*
▪ Default Precedence: Local → Site → Domain → OU → OU... (LSDOU)
▪ Seen on the Group Policy Inheritance tab
• Link order (attribute of GPO Link)
▪ Lower number → Higher on list → Precedent
• Block Inheritance (attribute of OU)
▪ Blocks the processing of GPOs from above
• Enforced (attribute of GPO Link)
▪ Enforced GPOs "blast through" Block Inheritance
▪ Enforced GPO settings win over conflicting settings in lower GPOs

A policy setting can be configured in more than one GPO, and GPOs can be in conflict with one another. For example, a policy setting can be enabled in one GPO, disabled in another GPO, and not configured in a third GPO. In this case, the precedence of the GPOs determines which policy setting the client applies. A GPO with higher precedence prevails over a GPO with lower precedence. Precedence is shown as a number in the GPMC. The smaller the number—that is, the closer to 1—the higher the precedence, so a GPO with a precedence of 1 will prevail over other GPOs. Select the domain or OU and then click the **Group Policy Inheritance** tab to view the precedence of each GPO.

When a policy setting is enabled or disabled in a GPO with higher precedence, the configured setting takes effect. However, remember that policy settings are set to Not Configured by default. If a policy setting is not configured in a GPO with higher precedence, the policy setting (either enabled or disabled) in a GPO with lower precedence will take effect.

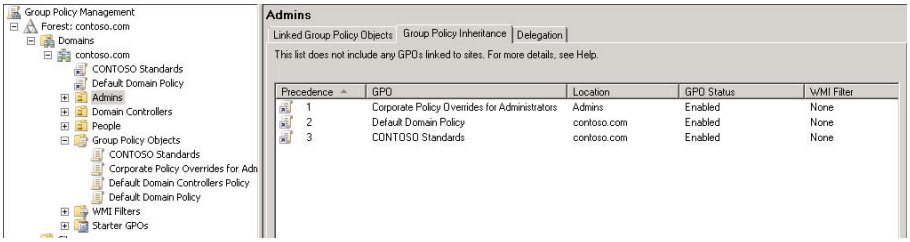
A site, domain, or OU can have more than one GPO linked to it. The link order of GPOs determines the precedence of GPOs in such a scenario. GPOs with a higher-link order take precedence over GPOs with a lower-link order. When you select an OU in the GPMC, the Linked Group Policy Objects tab shows the link order of GPOs linked to that OU.

The default behavior of Group Policy is that GPOs linked to a higher-level container are inherited by lower-level containers. When a computer starts up or a user logs on, the Group Policy Client examines the location of the computer or user object in Active Directory and evaluates the GPOs with scopes that include the computer or user. Then, the client-side extensions apply policy settings from these GPOs. Policies are applied sequentially, beginning with the policies linked to the site, followed by those linked to the domain, followed by those linked to OUs—from the top-level OU down to the OU in which the user or computer object exists. It is a layered application of settings, so a GPO that is applied later in the process, because it has higher precedence, overrides settings applied earlier in the process.

The sequential application of GPOs creates an effect called policy inheritance. Policies are inherited, so the resultant set of group policies for a user or computer will be the cumulative effect of site, domain, and OU policies.

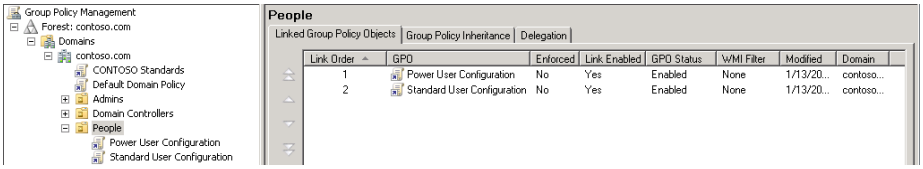
MCT USE ONLY. STUDENT USE PROHIBITED

By default, inherited GPOs have lower precedence than GPOs linked directly to the container. For example, you might configure a policy setting to disable the use of registry-editing tools for all users in the domain by configuring the policy setting in a GPO linked to the domain. That GPO, and its policy setting, is inherited by all users within the domain. However, you probably want administrators to be able to use registry-editing tools, so you will link a GPO to the OU that contains administrators' accounts and configure the policy setting to allow the use of registry-editing tools. Because the GPO linked to the administrators' OU takes higher precedence than the inherited GPO, administrators will be able to use registry-editing tools. The following figure illustrates Group Policy Inheritance:




## Precedence of Multiple Linked GPOs

An OU, domain, or site can have more than one GPO linked to it. If there are multiple GPOs, the objects' link order determines their precedence. In the following figure, two GPOs are linked to the People OU:




The object higher on the list, with a link order of 1, has the highest precedence. Therefore, settings that are enabled or disabled in the Power User Configuration

PO has precedence over the same settings in the Standard User Configuration GPO.

To change the precedence of a GPO link:

1. Select the OU, site, or domain in the GPMC console tree.
2. Click the **Linked Group Policy Objects** tab in the details pane.
3. Select the GPO.
4. Use the **Up**, **Down**, **Move To Top**, and **Move To Bottom** arrows to change the link order of the selected GPO.

## Block Inheritance

A domain or OU can be configured to prevent the inheritance of policy settings.

To block inheritance, right-click the domain or OU in the GPMC console tree and select Block Inheritance.

The Block Inheritance option is a property of a domain or OU, so it blocks all Group Policy settings from GPOs linked to parents in the Group Policy hierarchy. When you block inheritance on an OU, for example, GPO application begins with any GPOs linked directly to that OU—GPOs linked to higher-level OUs, the domain, or the site will not apply.

MCT USE ONLY. STUDENT USE PROHIBITED

The Block Inheritance option should be used sparingly. Blocking inheritance makes it more difficult to evaluate Group Policy precedence and inheritance. In a later topic, you will learn how to scope a GPO so that it applies to only a subset of objects -or so that it is prevented from applying to a subset of objects. With security group filtering, you can carefully scope a GPO so that it applies to only the correct users and computers in the first place, making it unnecessary to use the Block Inheritance option.

## Enforce a GPO Link

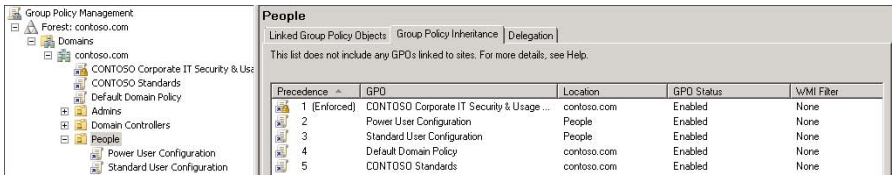
In addition, a GPO link can be set to Enforced.

To enforce a GPO link, right-click the GPO link in the console tree and choose **Enforced** from the context menu.

When a GPO link is set to **Enforced**, the GPO takes the highest level of precedence; policy settings in that GPO will prevail over any conflicting policy settings in other GPOs. In addition, a link that is enforced will apply to child containers even when those containers are set to Block Inheritance. The **Enforced** option causes the policy to apply to all objects within its scope. Enforced will cause policies to override any conflicting policies and will apply regardless of whether a Block Inheritance option is set.

In the figure on the following page, Block Inheritance has been applied to the Business OU. As a result, GPO D, which is applied to the domain, is blocked and does not apply when a user from the Employees OU logs on to a computer in the Clients OU. However, in the Security GPO, GPOs linked to the domain with the **Enforced** option does apply. In fact, it is applied last in the processing order, meaning its settings will override those of GPOs B, C, and E.

When you configure a GPO that defines configuration mandated by your corporate IT security and usage policies, you want to ensure that those settings are not overridden by other GPOs. You can do this by enforcing the link of the GPO. The figure here shows just this scenario:



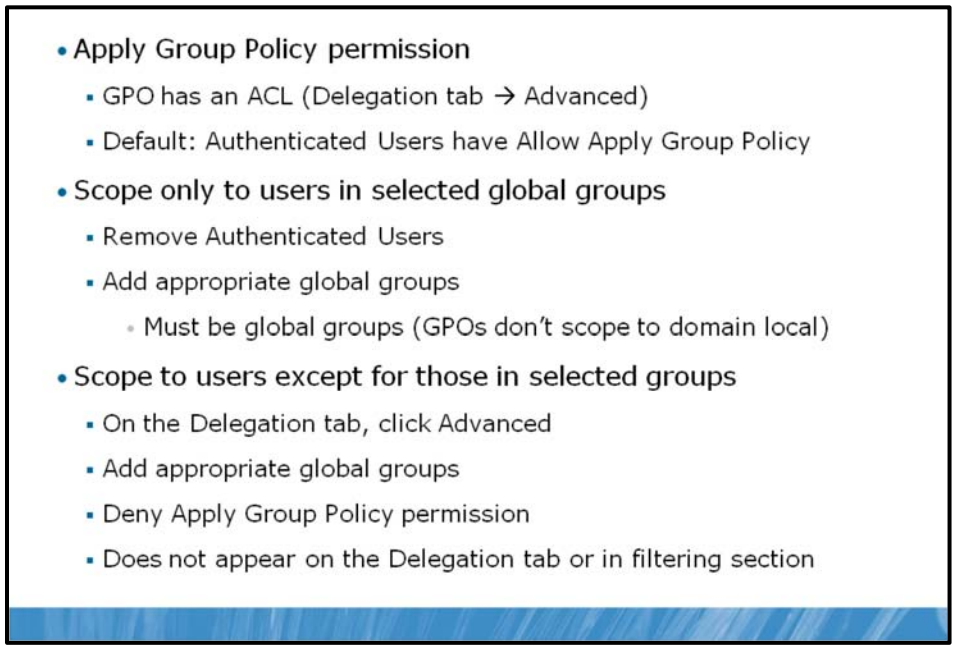

Configuration mandated by corporate policies is deployed in the CONTOSO Corporate IT Security & Usage GPO, which is linked with an enforced link to the Contoso.com domain. The icon for the GPO link has a padlock on it—the visual indicator of an enforced link. On the People OU, the **Group Policy Inheritance** tab shows that the GPO takes precedence even over the GPOs linked to the People OU itself.

## Evaluating Precedence

To facilitate evaluation of GPO precedence, you can simply select an OU (or domain) and click the **Group Policy Inheritance** tab. This tab will display the resulting precedence of GPOs, accounting for GPO link, link order, inheritance blocking, and link enforcement. This tab does not account for policies that are linked to a site, nor does it account for GPO security or WMI filtering.

MCT USE ONLY. STUDENT USE PROHIBITED

## Use Security Filtering to Modify GPO Scope


Apply Group Policy permission
GPO has an ACL (Delegation tab → Advanced)
Default: Authenticated Users have Allow Apply Group Policy
Scope only to users in selected global groups
Remove Authenticated Users
Add appropriate global groups
Must be global groups (GPOs don't scope to domain local)
Scope to users except for those in selected groups
On the Delegation tab, click Advanced
Add appropriate global groups
Deny Apply Group Policy permission
Does not appear on the Delegation tab or in filtering section

By now, you've learned that you can link a GPO to a site, domain, or OU. However, you might need to apply GPOs only to certain groups of users or computers rather than to all users or computers within the scope of the GPO. Although you cannot directly link a GPO to a security group, there is a way to apply GPOs to specific security groups. The policies in a GPO apply only to users who have Allow Read and Allow Apply Group Policy permissions to the GPO.

Each GPO has an ACL that defines permissions to the GPO. Two permissions, Allow Read and Allow Apply Group Policy, are required for a GPO to apply to a user or computer. For example, if a GPO is scoped to a computer by its link to the computer's OU, but the computer does not have Read and Apply Group Policy permissions, it will not download and apply the GPO. Therefore, by setting the appropriate permissions for security groups, you can filter a GPO so that its settings apply only to the computers and users you specify.

By default, Authenticated Users are given the Allow Apply Group Policy permission on each new GPO. This means that by default, all users and computers are affected by the GPOs set for their domain, site, or OU, regardless of the other groups in which they might be members. Therefore, there are two ways of filtering GPO scope:

- Remove the Apply Group Policy permission (currently set to Allow) for the Authenticated Users group but do not set this permission to Deny. Then, determine the groups to which the GPO should be applied and set the Read and Apply Group Policy permissions for these groups to Allow.
- Determine the groups to which the GPO should not be applied and set the Apply Group Policy permission for these groups to Deny. If you deny the Apply Group Policy permission to a GPO, the user or computer will not apply settings in the GPO, even if the user or computer is a member of another group that is allowed the Apply Group Policy Permission.

MCT USE ONLY. STUDENT USE PROHIBITED

## Filtering a GPO to Apply to Specific Groups

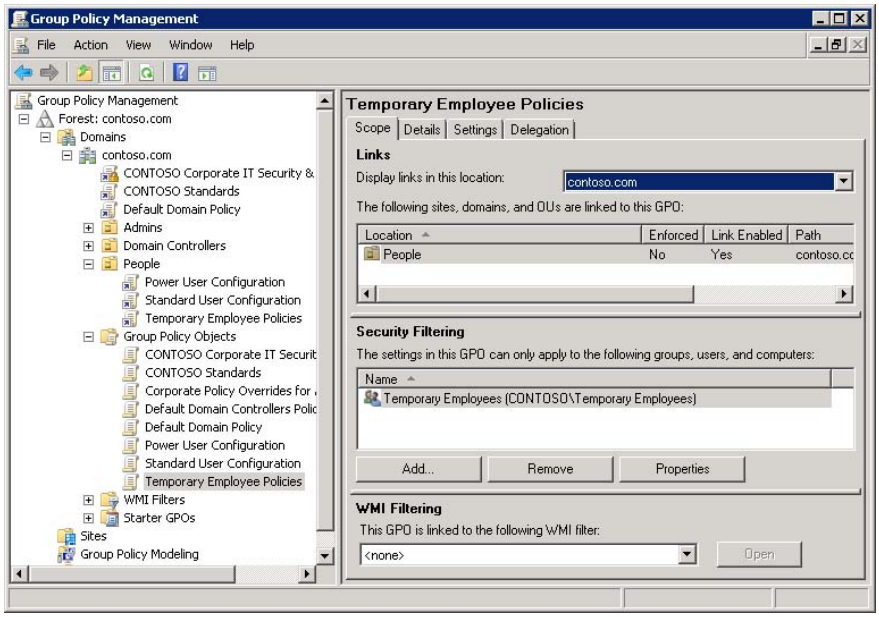
To apply a GPO to a specific security group:

1. Select the GPO in the **Group Policy Objects** container in the console tree.
2. In the **Security Filtering** section, select the **Authenticated Users** group and click **Remove**.

**Note** GPOs can be filtered only with global security groups; not with domain local security groups.

3. Click **OK** to confirm the change.
4. Click **Add**.
5. Select the group to which you want the policy to apply and click **OK**.

The result will look similar to the figure shown here—the Authenticated Users group is not listed, and the specific group to which the policy should apply is listed.




## Filtering a GPO to Exclude Specific Groups

The **Scope** tab of a GPO does not allow you to exclude specific groups. To exclude a group—that is, to deny the Apply Group Policy permission—you must use the **Delegation** tab.

To deny a group the Apply Group Policy permission:

1. Select the GPO in the **Group Policy Objects** container in the console tree.
2. Click the **Delegation** tab.
3. Click the **Advanced** button.

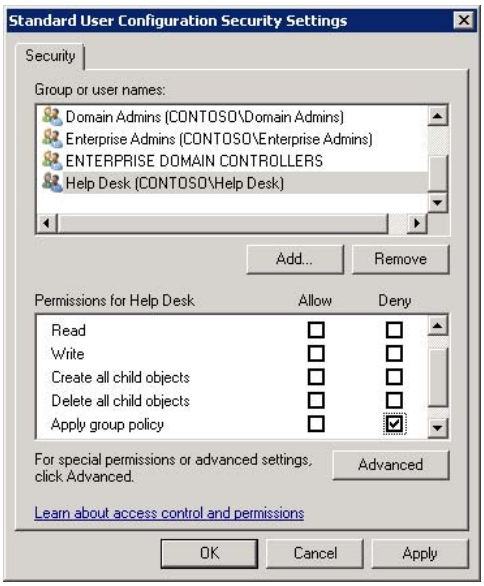
   The **Security Settings** dialog box appears.
4. Click the **Add** button.

MCT USE ONLY. STUDENT USE PROHIBITED

5. Select the group you want to exclude from the GPO. Remember, it must be a global group. GPO scope cannot be filtered by domain local groups.
6. Click **OK**.

   The group you selected is given the Allow Read permission by default.
7. Clear the **Allow Read permission** check box.
8. Select the **Deny Apply Group Policy** check box.

The figure here shows an example that denies the Help Desk group the Apply group policy permission and, therefore, excludes the group from the scope of the GPO.




9. Click **OK**.

You are warned that Deny permissions override other permissions.

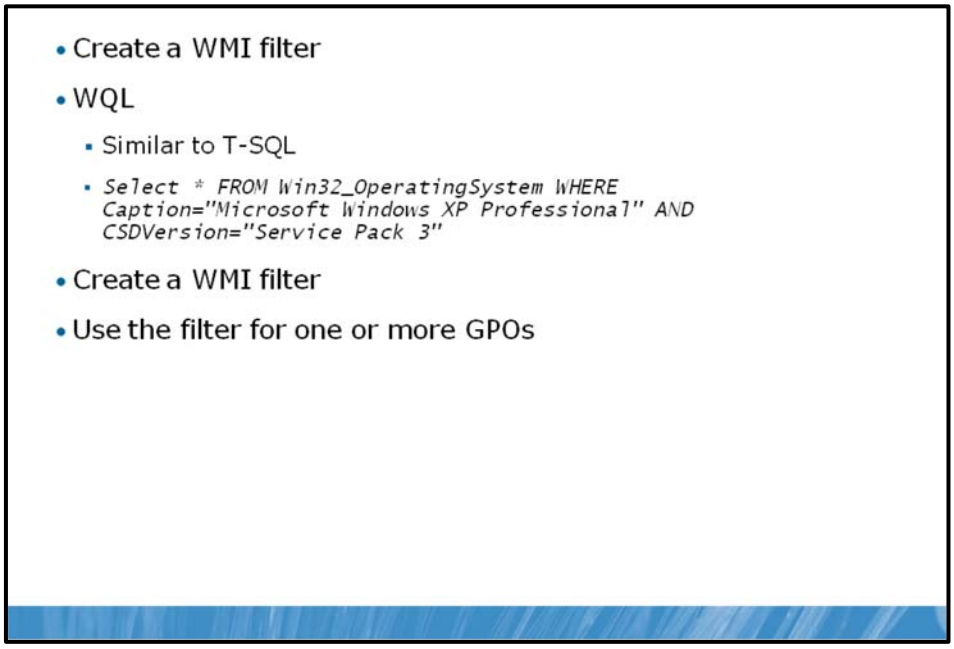
Because Deny permissions override Allow permissions, it is recommended that you use them sparingly. Microsoft Windows reminds you of this best practice with the warning message. The process to exclude groups with the Deny Apply Group Policy permission is far more laborious than the process to include groups in the Security Filtering section of the Scope tab.

10. Confirm that you want to continue.

**Important** Deny permissions are not exposed on the Scope tab. Unfortunately, when you exclude a group, the exclusion is not shown in the Security Filtering section of the **Scope** tab. This is yet one more reason to use Deny permissions sparingly.

MCT USE ONLY. STUDENT USE PROHIBITED

## WMI Filters


• Create a WMI filter
• WQL
• Similar to T-SQL
• Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft Windows XP Professional" AND CSDVersion="Service Pack 3"
• Create a WMI filter
• Use the filter for one or more GPOs

WMI is a management infrastructure technology that enables administrators to monitor and control managed objects in the network. A WMI query is capable of filtering systems based on characteristics, including RAM, processor speed, disk capacity, IP address, operating system version and service pack level, installed applications, and printer properties. Because WMI exposes almost every property of every object within a computer, the list of attributes that can be used in a WMI query is virtually unlimited. WMI queries are written by using WMI Query Language (WQL).

You can use a WMI query to create a WMI filter, with which a GPO can be filtered. A good way to understand the purpose of a WMI filter, both for the certification exams and for real-world implementation, is through examples. Group Policy can be used to deploy software applications and service packs—a capability that is discussed in Module 7. You might create a GPO to deploy an application and then use a WMI filter to specify that the policy should apply only to computers with a certain operating system and service pack–Windows XP SP3, for example. The WMI query to identify such systems is:

```
Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft
Windows XP Professional" AND CSDVersion="Service Pack 3"
```

When the Group Policy Client evaluates GPOs it has downloaded to determine which should be handed off to the CSEs for processing, it performs the query against the local system. If the system meets the criteria of the query, the query result is a logical True, and the CSEs process the GPO.

WMI exposes namespaces, within which are classes that can be queried. Many useful classes, including Win32_Operating System, are found in a class called root\CIMv2.

To create a WMI filter:

1. Right-click the **WMI Filters** node in the GPMC console tree, and then click **New**.

   Type a name and description for the filter, and then click the **Add** button.

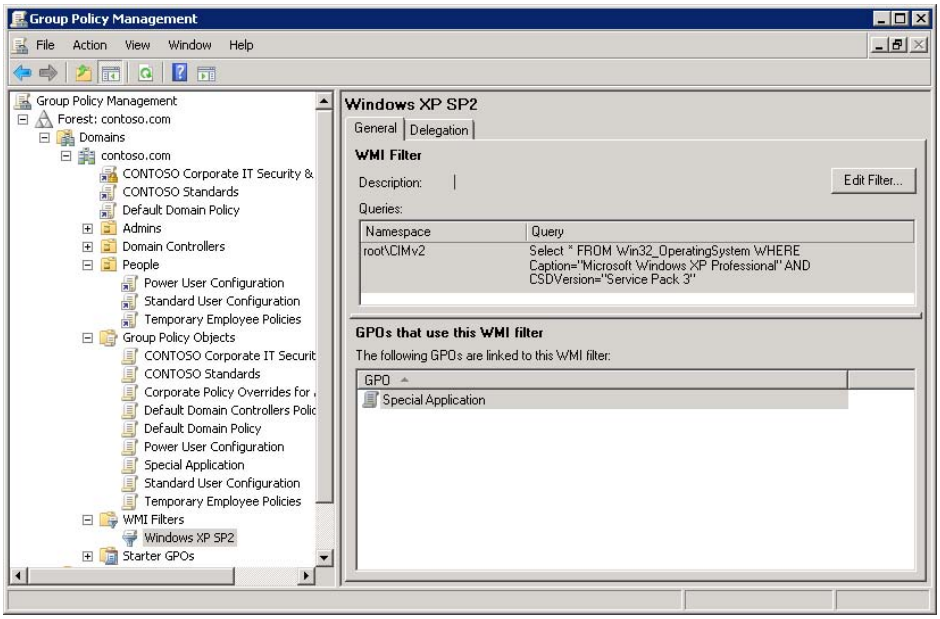
MCT USE ONLY. STUDENT USE PROHIBITED

2. In the **Namespace** box, type the namespace for your query.
3. In the **Query** box, enter the query.
4. Click **OK**.

To filter a GPO with a WMI filter:

1. Select the GPO or GPO link in the console tree.
2. Click the **Scope** tab.
3. Click the WMI drop-down list, and select the WMI filter.

A GPO can be filtered by only one WMI filter, but that WMI filter can be a complex query that uses multiple criteria. A single WMI filter can be linked to, and thereby used to filter, one or more GPOs. The **General** tab of a WMI filter, shown in the figure here, displays the GPOs that use the WMI filter:




There are three significant caveats regarding WMI filters.

- First, the WQL syntax of WMI queries can be challenging to master. You can often find examples on the Internet when you search by using the keywords *WMI filter* and *WMI query*, along with a description of the query you want to create.
- Second, WMI filters are expensive in terms of Group Policy processing performance. Because the Group Policy Client must perform the WMI query at each policy processing interval, there is a slight impact on system performance every 90–120 minutes. With the performance of today's computers, the impact might not be noticeable, but you should certainly test the effects of a WMI filter prior to deploying it widely in your production environment.

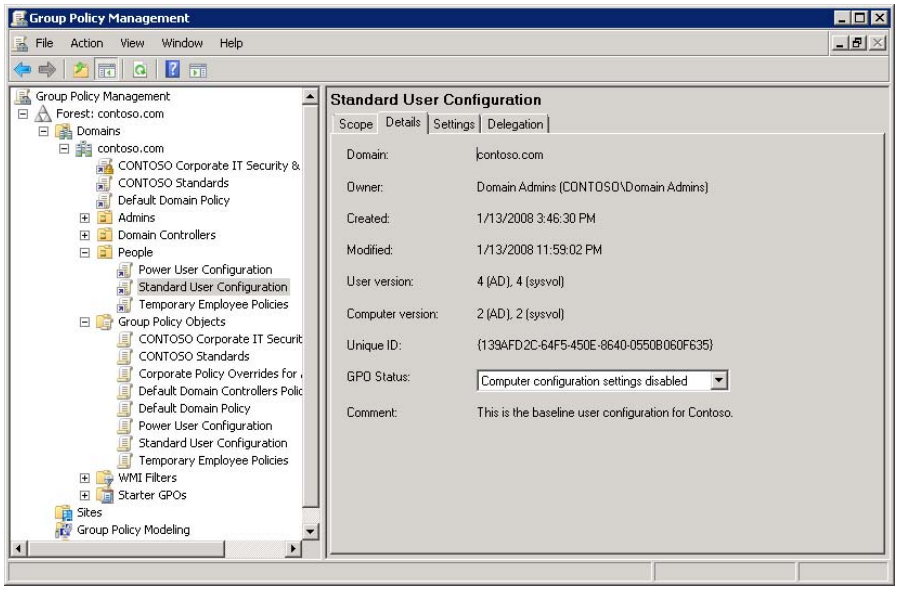
  Note that the WMI query is processed only *one* time, even if it is used to filter the scope of multiple GPOs.
- Third, WMI filters are not processed by computers running Windows 2000 Server. If a GPO is filtered with a WMI filter, a Windows 2000 Server system ignores the filter and processes the GPO as if the results of the filter were true.

MCT USE ONLY. STUDENT USE PROHIBITED

## Enable or Disable GPOs and GPO Nodes

- GPO Details tab → GPO Status drop-down list
- Enabled: Both Computer Configuration and User Configuration settings will be applied by CSEs
- All settings disabled: CSEs will not process the GPO
- Computer Configuration settings disabled: CSEs will not process settings in Computer Configuration
- User Configuration settings disabled: CSEs will not process settings in User Configuration

You can prevent the settings in the Computer Configuration or User Configuration nodes from being processed during policy refresh by changing the GPO Status.




To enable or disable a GPO's nodes, select the GPO or GPO link in the console tree, click the **Details** tab, shown in the figure, and then select one of the following from the GPO Status drop-down list :

- **Enabled.** Both computer configuration settings and user configuration settings will be processed by CSEs during policy refresh.
- **All Settings Disabled.** CSEs will not process the GPO during policy refresh.

MCT USE ONLY. STUDENT USE PROHIBITED

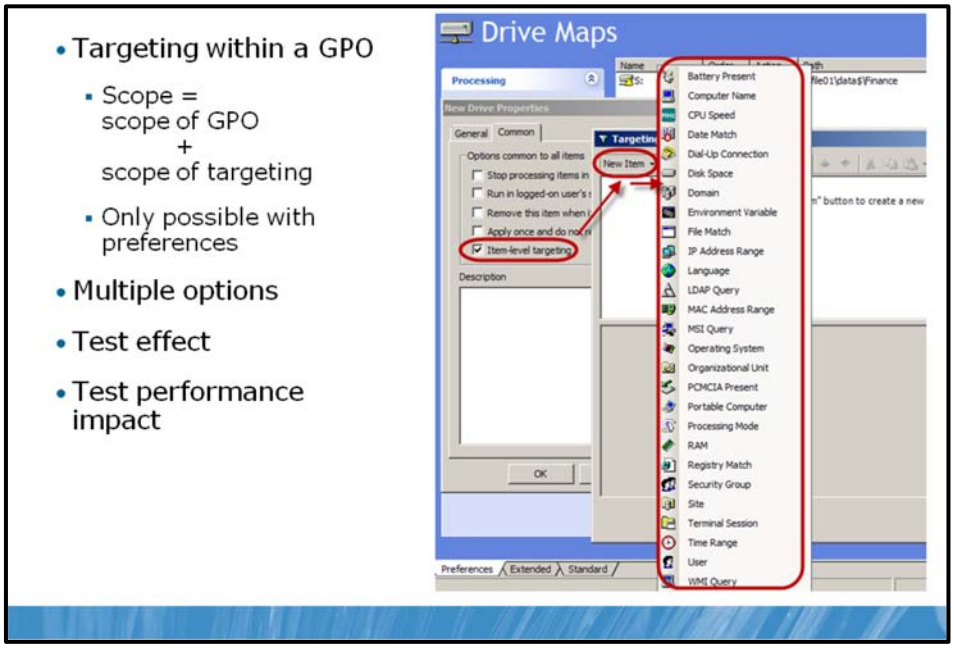
- **Computer Configuration Settings Disabled.** During computer policy refresh, computer configuration settings in the GPO will not be applied.
- **User Configuration Settings Disabled.** During user policy refresh, user configuration settings in the GPO will not be applied.

You can configure GPO status to optimize policy processing. If a GPO contains only user settings, for example, setting the GPO Status option to disable computer settings prevents the Group Policy client from attempting to process the GPO during computer policy refresh. Because the GPO contains no computer settings, there is no need to process the GPO, and you can save a few cycles of the processor.

**Note** You can define a configuration that should take effect in case of an emergency, security incident, or other disasters in a GPO and link the GPO so that it is scoped to appropriate users and computers. Then, disable the GPO. If you require the configuration to be deployed, enable the GPO.

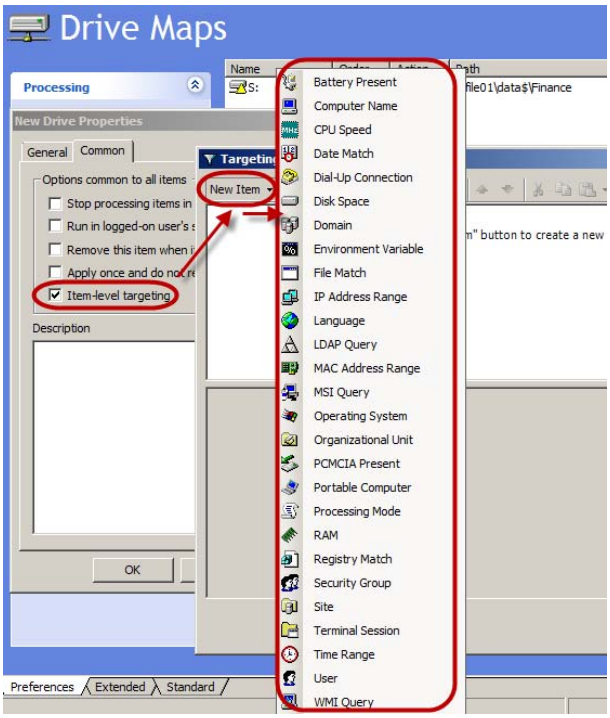
MCT USE ONLY. STUDENT USE PROHIBITED

## Target Preferences




Preferences, which are new to Windows Server 2008, have a built-in scoping mechanism called item-level targeting. You can have multiple preference items in a single GPO, and each preference item can be targeted or filtered. So, for example, you could have a single GPO with a preference that specifies folder options for engineers and another item that specifies folder options for sales people. You can target the items by using a security group or OU. There are over a dozen other criteria that can be used, including hardware and network characteristics, date and time, Lightweight Directory Access Protocol (LDAP) queries, and more.

MCT USE ONLY. STUDENT USE PROHIBITED

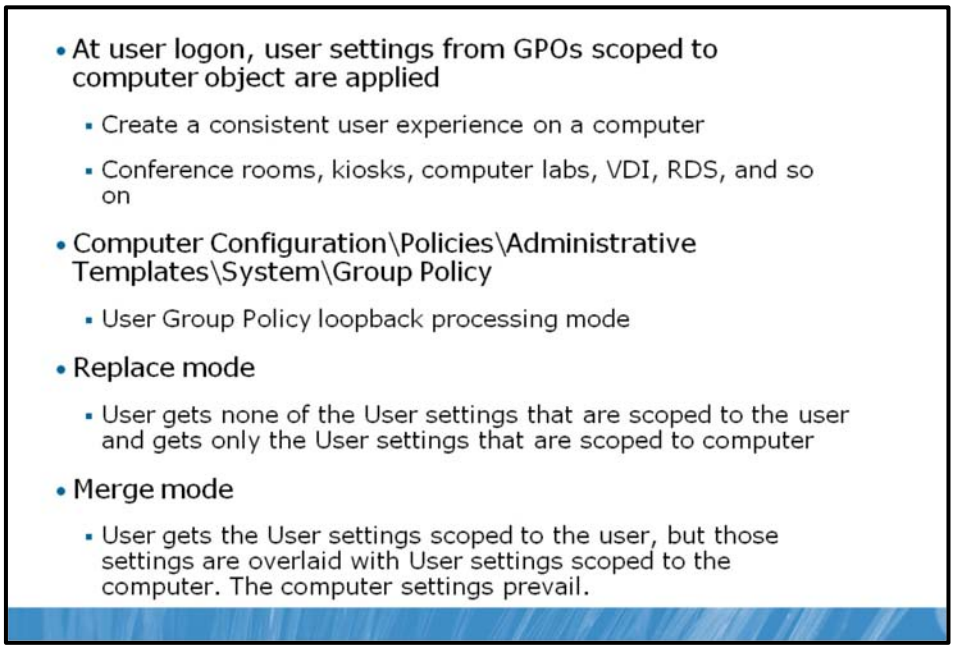



**Note** What's new about preferences is that you can target multiple preference items within a single GPO instead of requiring multiple GPOs. With traditional policies, you often need multiple GPOs filtered to individual groups to apply variations of settings.

Like WMI filters, item-level targeting of preferences requires the CSE to perform a query to determine whether to apply the settings in a preferences item. You must be aware of the potential performance impact of item-level targeting, particularly if you use options such as LDAP queries, which require processing time and a response from a domain controller to process. As you design your Group Policy infrastructure, balance the configuration management benefits of item-level targeting against the performance impact you discover during testing in a lab.

MCT USE ONLY. STUDENT USE PROHIBITED

## Loopback Policy Processing


At user logon, user settings from GPOs scoped to computer object are applied
Create a consistent user experience on a computer
Conference rooms, kiosks, computer labs, VDI, RDS, and so on
Computer Configuration\Policies\Administrative Templates\System\Group Policy
User Group Policy loopback processing mode
Replace mode
User gets none of the User settings that are scoped to the user and gets only the User settings that are scoped to computer
Merge mode
User gets the User settings scoped to the user, but those settings are overlaid with User settings scoped to the computer. The computer settings prevail.

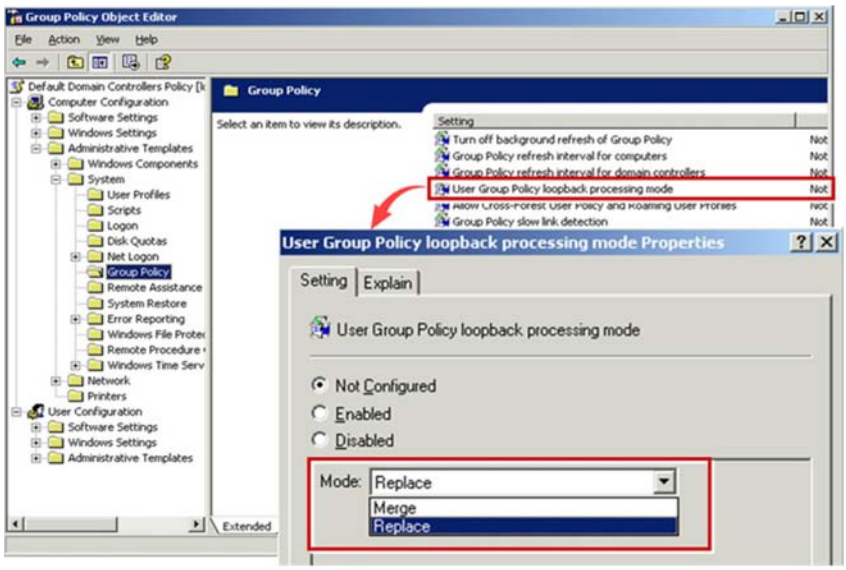
By default, a user's settings come from GPOs scoped to the user object in Active Directory. Regardless of which computer the user logs on to, the resultant set of policies that determine the user's environment is the same. There are situations, however, in which you might want to configure a user differently, depending on the computer in use. For example, you might want to lock down and standardize user desktops when users log on to computers in closely managed environments such as conference rooms, reception areas, laboratories, classrooms, and kiosks. It is also important for virtual desktop infrastructure (VDI) scenarios, including remote virtual machines and Remote Desktop Services (RDS), known as Terminal Services in previous versions.

Imagine a scenario in which you want to enforce a standard corporate appearance for the Windows desktop on all computers in conference rooms and other public areas of your office. How will you centrally manage this configuration by using Group Policy? Policy settings that configure desktop appearance are located in the User Configuration node of a GPO. Therefore, by default, the settings apply to users, regardless of which computer they log on to. The default policy processing does not give you a way to scope user settings to apply to computers, regardless of which user logs on. That's where loopback policy processing comes in.

Loopback policy processing alters the default algorithm used by the Group Policy client to obtain the ordered list of GPOs that should be applied to a user's configuration. Instead of user configuration being determined by the User Configuration node of GPOs that are scoped to the user object, user configuration can be determined by the User Configuration node policies of GPOs that are scoped to the computer object.

The User Group Policy loopback processing mode policy, located in the Computer Configuration\Policies\Administrative Templates\System\Group Policy folder in GPME, can be, like all policy settings, set to **Not Configured**, **Enabled**, or **Disabled**.

MCT USE ONLY. STUDENT USE PROHIBITED



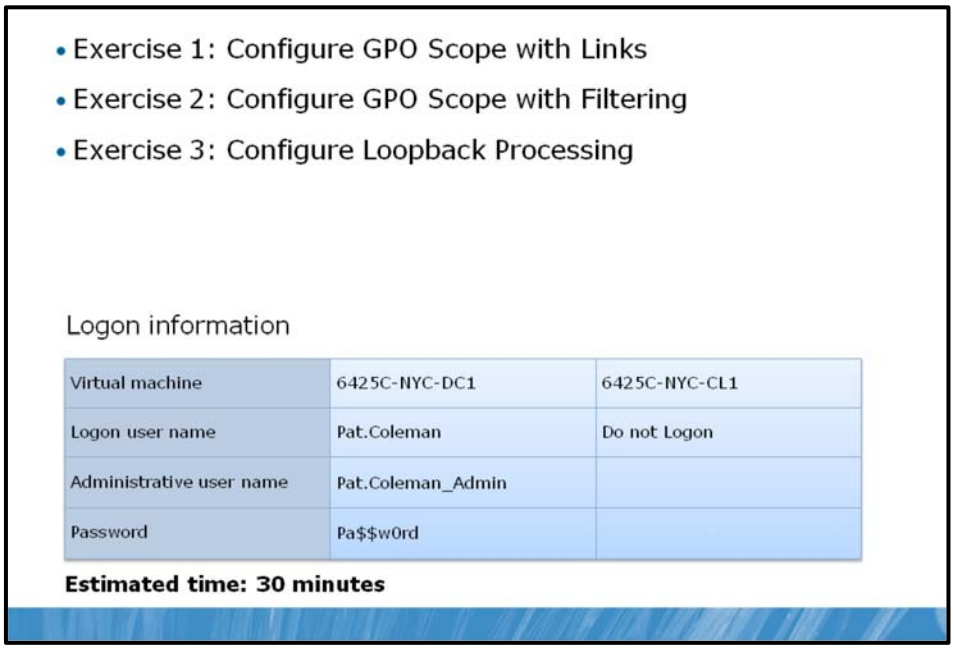

When enabled, the policy can specify the **Replace** or **Merge** mode.

- **Replace.** In this case, the GPO list for the user (obtained in step 5 in the "Group Policy Processing," the next section) is replaced entirely by the GPO list already obtained for the computer at computer startup (in step 2). The settings in User Configuration policies of the computer's GPOs are applied to the user. The Replace mode is useful in a situation such as a classroom where users should receive a standard configuration rather than the configuration applied to those users in a less managed environment.
- **Merge.** In this case, the GPO list obtained for the computer at computer startup (step 2 in the "Group Policy Processing" section) is appended to the GPO list obtained for the user when logging on (step 5). Because the GPO list obtained for the computer is applied later, settings in GPOs on the computer's list have precedence if they conflict with settings in the user's list. This mode would be useful to apply additional settings to users' typical configurations. For example, you might allow a user to receive the user's typical configuration when logging on to a computer in a conference room or reception area, but replace the wallpaper with a standard bitmap and disable the use of certain applications or devices.

**Note** It is a less documented fact that when you combine the loopback processing with security group filtering, the application of user settings during policy refresh uses the credentials of the computer to determine which GPOs to apply as part of the loopback processing. However, the logged-on user must also have the Apply Group Policy permission for the GPO to be successfully applied.

MCT USE ONLY. STUDENT USE PROHIBITED

# Lab B: Manage Group Policy Scope




## Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **6425C-NYC-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
   - User name: **Pat.Coleman**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
5. Start 6425C-NYC-CL1. Do not log on to the client computer until directed to do so.

## Lab Scenario

You are an administrator of thecontoso.com domain. The Contoso Standards GPO, linked to the domain, configures a policy setting that requires a ten-minute screen saver timeout. An engineer reports that a critical application that performs lengthy calculations crashes when the screens saver starts, and the engineer has asked you to prevent the setting from applying to the team of engineers that uses the application every day. You have also been asked to configure conference room computers to use a 45-minute timeout so that the screen saver does not launch during a meeting.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 1: Configure GPO Scope with Links

In this exercise, you will modify the scope of GPOs by using GPO links, and you will explore inheritance, precedence, and the effects of Enforced links and Block Inheritance.

The main tasks for this exercise are as follows:

1. Create a GPO with a policy setting that takes precedence over a conflicting setting.
2. View the effect of an enforced GPO link.
3. Apply Block Inheritance.

### ▶ Task 1: Create a GPO with a policy setting that takes precedence over a conflicting setting.

1. On NYC-DC1, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. In the **User Accounts\Employees** OU, create a sub-OU called **Engineers**, and then close Active Directory Users and Computers.
3. Run the Group Policy Management Console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
4. Create a new GPO linked to the **Engineers** OU called **Engineering Application Override**.
5. Configure the **Screen saver timeout** policy setting to be disabled, and then close the GPME.
6. Select the **Engineers** OU, and then click the **Group Policy Inheritance** tab. Notice that the **Engineering Application Override** GPO has precedence over the **CONTOSO Standards** GPO. The screen saver timeout policy setting you just configured in the **Engineering Application Override** GPO will be applied after the setting in the **CONTOSO Standards** GPO**.** Therefore, the new setting will overwrite the standards setting, and will "win." Screen saver timeout will be disabled for users within the scope of the **Engineering Application Override** GPO.

### ▶ Task 2: View the effect of an enforced GPO link.

1. In the GPMC console tree, select the **Domain Controllers** OU, and then click the **Group Policy Inheritance** tab.
2. Notice that the GPO named **6425C** has the highest precedence. Settings in this GPO will override any conflicting settings in any of the other GPOs.

   The Default Domain Controllers GPO specifies, among other things, which groups are given the right to log on locally to domain controllers. To enhance the security of domain controllers, standard users are not given the right to log on locally. to allow a nonprivileged user account such as Pat.Coleman to log on to domain controllers. In this course, the 6425C GPO gives Domain Users the right to log on locally to a computer. The 6425C GPO is linked to the domain, so its settings would normally be overridden by settings in the Default Domain Controllers GPO. Therefore, the 6425C GPO link to the domain is configured as Enforced. In this way, the conflict in user rights assignment between the two GPOs is "won" by the 6425C GPO.

### ▶ Task 3: Apply Block Inheritance.

1. In the GPMC console, select the **Engineers** OU and examine the precedence and inheritance of GPOs on the **Group Policy Inheritance** tab.
2. Block the inheritance of GPOs to the **Engineers** OU.

**Question:** Which GPOs continue to apply to users in the Engineers OU? Where are those GPOs linked? Why did they continue to apply?

3. Turn off **Block Inheritance** from the **Engineers** OU.

**Results:** In this exercise, you created a GPO called Engineering Application Override and linked it to the Engineers OU. You also have an understanding of inheritance, precedence, and the effects of an Enforced link and Block Inheritance.

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 2: Configure GPO Scope with Filtering

As time passes, you discover that only a small number of engineers require the screen saver timeout override that is currently applied to all users in the Engineers OU. In addition, you discover that a few users must be exempted from the screen saver timeout policy and other settings configured by the CONTOSO Standards GPO. You decide to use security filtering to manage the scope of the GPOs.

In this exercise, you will modify the scope of GPOs by using filtering.

The main tasks for this exercise are as follows:

1. Configure policy application with security filtering.
2. Configure an exemption with security filtering.

▶ Task 1: Configure policy application with security filtering.

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. In the **Groups\Configuration** OU, create a global security group named **GPO_Engineering Application Override_Apply**.
3. In the GPMC console, select the **Engineering Application Override** GPO. Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
4. Configure the GPO to apply only to the **GPO_Engineering Application Override_Apply** group.

▶ Task 2: Configure an exemption with security filtering.

1. Run **Active Directory Users and Computers** as an administrator with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. In the **Groups\Configuration** OU**,** create a global security group named **GPO_CONTOSO Standards_Exempt**.
3. In the GPMC console, select the **CONTOSO Standards** GPO**.** Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
4. Configure the GPO to deny **Apply Group Policy** permission to the **GPO_CONTOSO Standards_Exempt** group.

**Results:** In this exercise, you configured the Engineering Application Override GPO to apply only to the members of GPO_Engineering Application Override_Apply. You also configured a group with the Deny Apply Group Policy permission, which overrides the Allow permission. If any user requires exemption from the policies in the CONTOSO Standards GPO, you can simply add the computer to the group GPO_CONTOSO Standards_Exempt.

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 3: Configure Loopback Processing

You need to configure the screen saver timeout in conference rooms to 45 minutes so that a screen saver does not appear in the middle of a meeting.

In this exercise, you will configure loopback GPO processing.

The main task for this exercise is as follows:

- Configure loopback processing.

▶ Task 1: Configure loopback processing.

1. Create a new GPO named **Conference Room Policies** and link it to the **Kiosks\Conference Rooms** OU.
2. Confirm that the **Conference Room Policies** GPO is scoped to **Authenticated Users.**
3. Modify the **Screen Saver timeout** policy to launch the screen saver after 45 minutes. Modify the **User Group Policy loopback processing mode** policy setting to use **Merge** mode.

**Results:** In this exercise, you created a Conference Room Policies GPO that applies a 45-minute screen saver timeout to users when they log on to conference room computers.

**Note** Do not shut down the virtual machines after you finish this lab because the settings you have configured here will be used in subsequent labs.

### Lab Review Questions

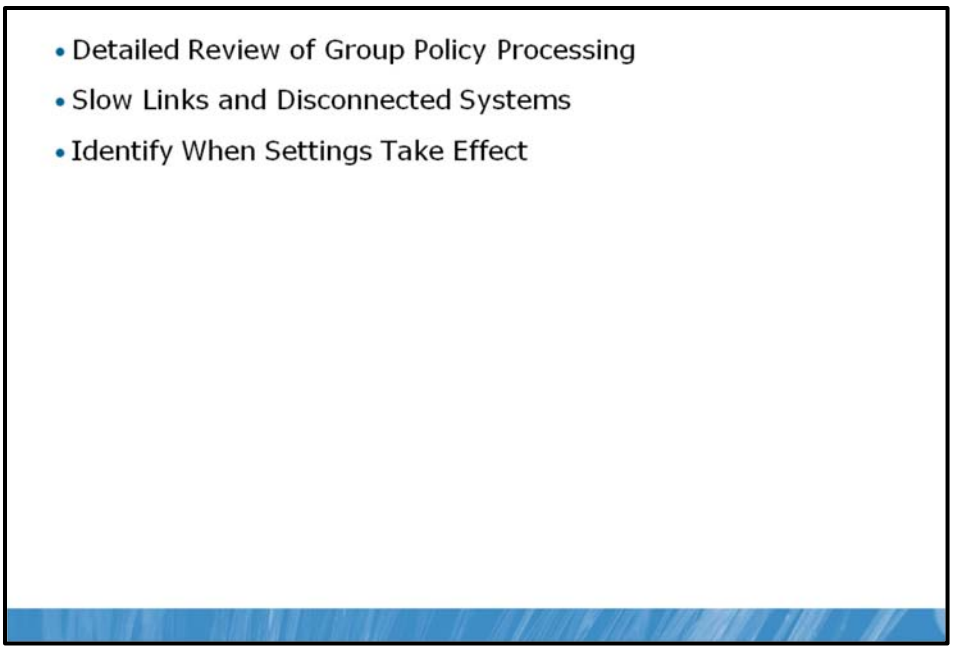
**Question:** Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs are typically linked very high in the Active Directory logical structure—to the domain itself or to a first-level OU. What advantages are gained by using security group filtering rather than GPO links to manage the scope of the GPO?

**Question:** Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO you create?

**Question:** Do you use loopback policy processing in your organization? In which scenarios and for which policy settings can loopback policy processing add value?

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 4
# Group Policy Processing




Now that you have learned more about the concepts, components, and scoping of Group Policy, you are ready to examine Group Policy processing closely.

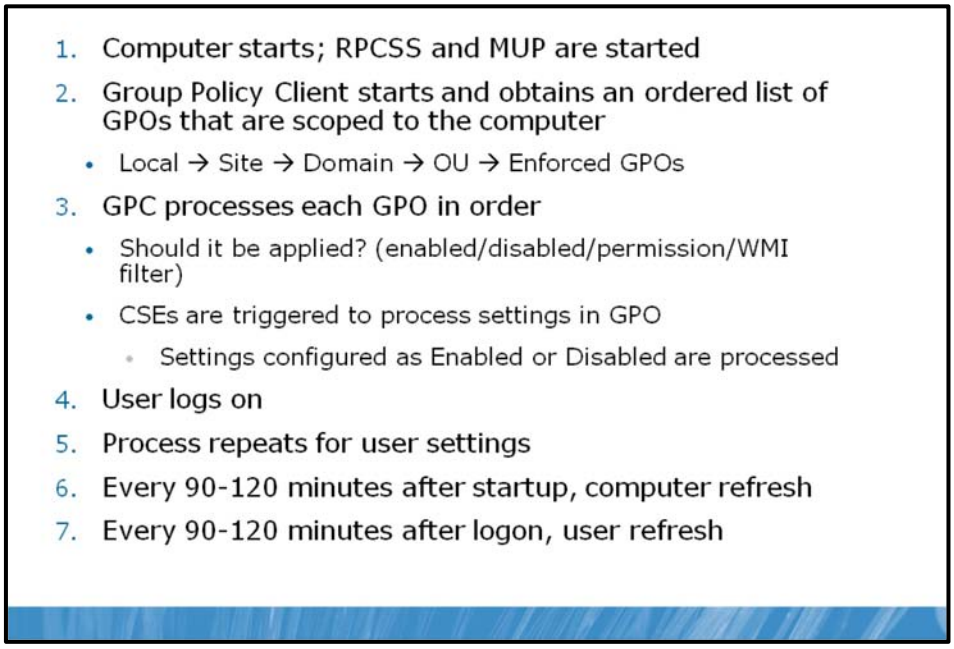
### Objectives

After completing this lesson, you will be able to:

- Understand, improve, and manually trigger policy refresh.
- Implement loopback policy processing.

MCT USE ONLY. STUDENT USE PROHIBITED

## Detailed Review of Group Policy Processing


1. Computer starts; RPCSS and MUP are started
2. Group Policy Client starts and obtains an ordered list of GPOs that are scoped to the computer
• Local → Site → Domain → OU → Enforced GPOs
3. GPC processes each GPO in order
• Should it be applied? (enabled/disabled/permission/WMI filter)
• CSEs are triggered to process settings in GPO
◦ Settings configured as Enabled or Disabled are processed
4. User logs on
5. Process repeats for user settings
6. Every 90-120 minutes after startup, computer refresh
7. Every 90-120 minutes after logon, user refresh

This topic details Group Policy processing. As you read it, remember that Group Policy is all about applying configurations defined by GPOs, that GPOs are applied in an order (site, domain, and OU), and that GPOs applied later in the order have higher precedence; their settings, when applied, will override settings applied earlier. The following sequence details the process through which settings in a domain-based GPO are applied to affect a computer or user.

1. The computer starts, and the network starts. Remote Procedure Call System Service (RPCSS) and Multiple Universal Naming Convention Provider (MUP) are started. The Group Policy Client is started.
2. The Group Policy Client obtains an ordered list of GPOs scoped to the computer.

   The order of the list determines the order of GPO processing, which is, by default, local, site, domain, and OU.

   - Local GPOs. Each computer running Windows Server 2003, Windows XP, and Windows 2000 has exactly one GPO stored locally. Windows Vista, Windows Server 2008, and Windows 7 have multiple local GPOs. The precedence of local GPOs is discussed in the "Local GPOs" section in Lesson 2.
   - Site GPOs. Any GPOs that have been linked to the site are added to the ordered list next. When multiple GPOs are linked to a site, a domain, or an OU, the link order, configured on the **Scope** tab, determines the order in which they are added to the list. The GPO that is highest on the list, with the number closest to 1, has the highest precedence, and is added to the list last. It will, therefore, be applied last, and its settings will override those of the GPOs applied earlier.
   - Domain GPOs. Multiple domain-linked GPOs are added as specified by the link order.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

**Note** Domain-linked policies are not inherited by child domains. Policies from a parent domain are not inherited by a child domain. Each domain maintains distinct policy links. However, computers in several domains might be within the scope of a GPO linked to a site.

- OU GPOs. GPOs linked to the OU highest in the Active Directory hierarchy are added to the ordered list, followed by GPOs linked to its child OU, and so on. Finally, the GPOs linked to the OU that contains the computer are added. If several group policies are linked to an OU, they are added in the order specified by the link order.
- Enforced GPOs are added at the end of the ordered list, so their settings will be applied at the end of the process and will, therefore, override settings of GPOs earlier in the list and in the process. As a point of trivia, enforced GPOs are added to the list in the reverse order: OU, domain, and site. This is relevant when you apply corporate security policies in a domain-linked enforced GPO. That GPO will be at the end of the ordered list and will be applied last, so its settings will take precedence.

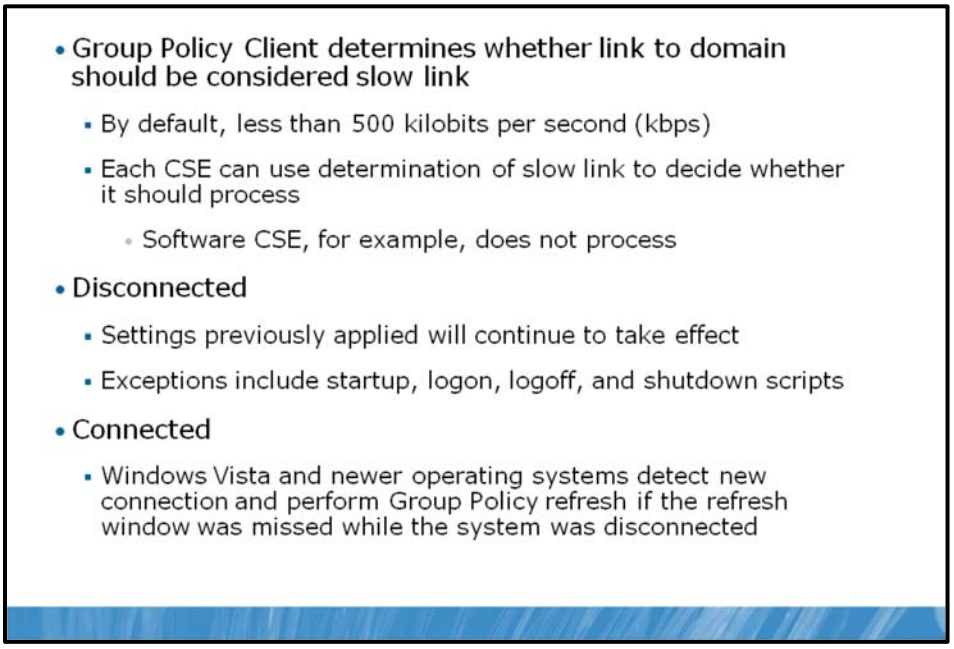
3. The GPOs are processed synchronously in the order specified by the ordered list. This means that settings in the local GPOs are processed first, followed by GPOs linked to the site, the domain, and the OUs containing the user or computer. GPOs linked to the OU of which the computer or user is a direct member are processed last, followed by enforced GPOs.
   - As each GPO is processed, the system determines whether its settings should be applied based on the GPO status for the computer node (enabled or disabled) and whether the computer has the Allow Group Policy permission. If a WMI filter is applied to the GPO, and if the computer is running Windows XP or later, it performs the WQL query specified in the filter.
4. If the GPO should be applied to the system, CSEs trigger to process the GPO settings. Policy settings in GPOs overwrite policies of previously applied GPOs in the following ways:
   - If a policy setting is configured (set to Enabled or Disabled) in a GPO linked to a parent container (OU, domain, or site), and the same policy setting is Not Configured in GPOs linked to its child container, the resultant set of policies for users and computers in the child container will include the parent's policy setting. If the child container is configured with the Block Inheritance option, the parent setting is not inherited unless the GPO link is configured with the Enforced option.
   - If a policy setting is configured (set to Enabled or Disabled) for a parent container, and the same policy setting is configured for a child, the child container's setting overrides the setting inherited from the parent. If the parent GPO link is configured with the Enforced option, the parent setting has precedence.
   - If a policy setting of GPOs linked to parent containers is Not Configured, and the child OU setting is also Not Configured, the resultant policy setting is the setting that results from the processing of local GPOs. If the resultant setting of local GPOs is also Not Configured, the resultant configuration is the Windows default setting.
5. When the user logs on, the process is repeated for user settings. The client obtains an ordered list of GPOs scoped to the user, examines each GPO synchronously, and hands over GPOs that should be applied to the appropriate CSEs for processing. This step is modified if User Loopback Group Policy Processing is enabled. Loopback policy processing is discussed in the next topic.

**Note** Some Policy settings are in both Computer Configuration and User Configuration nodes. Most policy settings are specific to either the User Configuration or Computer Configuration node. A few settings appear in both nodes. Although in most situations, the setting in the Computer Configuration node overrides the setting in the User Configuration node, it is important to read the explanatory text accompanying the policy setting to understand the setting's effect and its application.

6. Every 90–120 minutes after computer startup, computer policy refresh occurs, and the process is repeated for computer settings.
7. Every 90–120 minutes after user logon, user policy refresh occurs, and the process is repeated for user settings.

MCT USE ONLY. STUDENT USE PROHIBITED

## Slow Links and Disconnected Systems


• Group Policy Client determines whether link to domain should be considered slow link
▪ By default, less than 500 kilobits per second (kbps)
▪ Each CSE can use determination of slow link to decide whether it should process
◦ Software CSE, for example, does not process
• Disconnected
▪ Settings previously applied will continue to take effect
▪ Exceptions include startup, logon, logoff, and shutdown scripts
• Connected
▪ Windows Vista and newer operating systems detect new connection and perform Group Policy refresh if the refresh window was missed while the system was disconnected

One of the tasks that can be automated and managed with Group Policy is software installation. In Module 7, you'll learn about Group Policy Software Installation (GPSI), which is provided by the software installation CSE. You can configure a GPO to install one or more software packages.

Imagine, however, that a user connects to your network over a slow connection. You would not want large software packages to be transferred over the slow link because performance would be problematic.

The Group Policy Client addresses this concern by detecting the speed of the connection to the domain and determining whether the connection should be considered a slow link. That determination is then used by each CSE to decide whether to apply settings. The software extension, for example, is configured to forgo policy processing so that software is not installed if a slow link is detected. By default, a link is considered to be slow if it is less than 500 kilobits per second (kbps).

If Group Policy detects a slow link, it sets a flag to indicate the slow link to the CSEs. The CSEs can then determine whether to process the applicable Group Policy settings. The default slow link speed is 500 kilobits per second (Kbps), but you can configure this. The following table describes the default behavior of the client-side extensions:

MCT USE ONLY. STUDENT USE PROHIBITED

| Client-Side Extension | Slow link processing | Can it be changed? |
|---|---|---|
| Registry policy processing | On | No |
| Internet Explorer maintenance | Off | Yes |
| Software Installation policy | Off | Yes |
| Folder Redirection policy | Off | Yes |
| Scripts policy | Off | Yes |
| Security policy | On | No |
| Internet Protocol Security (IPSec) policy | Off | Yes |
| Wireless policy | Off | Yes |
| EFS Recovery policy | On | Yes |
| Disk Quota policy | Off | Yes |

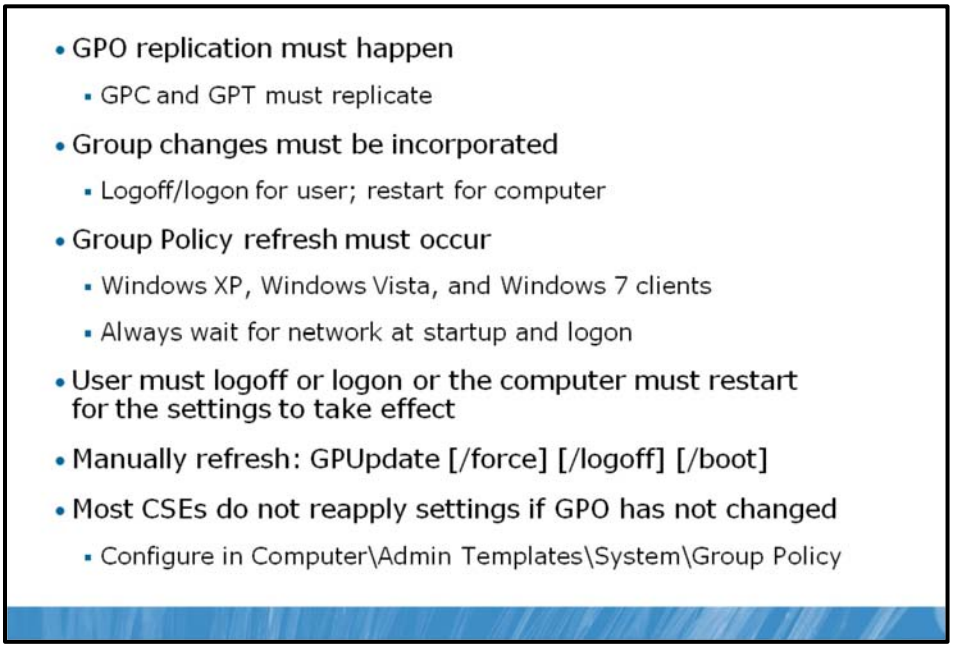
If a user is working while disconnected from the network, the settings previously applied by Group Policy continue to take effect, so a user's experience is identical, irrespective of whether he or she is on the network or away. There are exceptions to this rule, most notably that startup, logon, logoff, and shutdown scripts will not run if the user is disconnected.

If a remote user connects to the network, the Group Policy client wakes up and determines whether a Group Policy refresh window has been missed. If so, it performs a Group Policy refresh to obtain the latest GPOs from the domain. Again, the CSEs determine, based on their policy processing settings, whether settings in those GPOs are applied. This process does not apply to Windows XP or Windows Server 2003 systems. It applies only to Windows Vista, Windows Server 2008, Windows 7, and newer operating systems.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Identify When Settings Take Effect


• GPO replication must happen
▪ GPC and GPT must replicate
• Group changes must be incorporated
▪ Logoff/logon for user; restart for computer
• Group Policy refresh must occur
▪ Windows XP, Windows Vista, and Windows 7 clients
▪ Always wait for network at startup and logon
• User must logoff or logon or the computer must restart for the settings to take effect
• Manually refresh: GPUpdate [/force] [/logoff] [/boot]
• Most CSEs do not reapply settings if GPO has not changed
▪ Configure in Computer\Admin Templates\System\Group Policy

There are several processes that must be completed before Group Policy settings are actually applied to a user or a computer. We will discuss these processes in this topic

### GPO Replication Must Happen

Before a GPO can take effect, the Group Policy container (GPC) in Active Directory must be replicated to the domain controller from which the Group Policy Client obtains its ordered list of GPOs. Additionally, the Group Policy template (GPT) in SYSVOL must replicate to the same domain controller.

### Group Changes Must Be Incorporated

Finally, if you have added a new group or changed the membership of a group that is used to filter the GPO, that change must also be replicated, and the change must be in the security token of the computer and the user, which requires a restart (for the computer to update its group membership) or a logoff and logon (for the user to update its group membership).

### User or Computer Group Policy Refresh Must Occur

As you know, refresh happens at startup (for computer settings) and logon (for user settings) and every 90-120 minutes thereafter, by default.

**Note** Remember that the practical impact of the Group Policy refresh interval is that when you make a change in your environment, it will be on average one-half that time, or 45 to 60 minutes, before the change *starts* to take effect.

By default, Windows XP, Windows Vista, and Windows 7 clients perform only background refreshes at startup and logon, which means that a client might start up and a user might log on without receiving the latest policies from the domain. We highly recommend that you change this default behavior so that policy changes are implemented in a managed, predictable way. Enable the policy setting **Always Wait**

**For Network At Startup And Logon** for all Windows clients. The setting is located in Computer Configuration\Policies\Administrative Templates\System\Logon. Be sure to read the policy setting's explanatory text. Note that this does *not* affect the startup or logon time for computers that are not connected to a network. If the computer detects that it is disconnected, it does not "wait" for a network. The contoso.com domain used in this course has been preconfigured with this additional Group Policy setting.

### Settings Might Not Take Effect Immediately

Although most settings are applied during a background policy refresh, some CSEs do not apply the setting until the next startup or logon event. For example, newly added startup and logon script policies do not run until the next computer startup or logon. Software installation, which is discussed in Module 7, will occur at the next startup if the software is assigned in computer settings. Changes to folder redirection policies will not take effect until the next logon.

### Manually Refresh Group Policy with GPUpdate

When you are experimenting with Group Policy or trying to troubleshoot Group Policy processing, you might need to initiate a Group Policy refresh manually so that you do not have to wait for the next background refresh. The **GPUpdate** command can be used to initiate a Group Policy refresh. Used on its own, this command triggers processing identical to a background Group Policy refresh. Both computer policy and user policy are refreshed. Use the /target:computer or /target:user parameter to limit the refresh to computer or user settings, respectively. During background refresh, by default, settings are applied only if the GPO has been updated. The /force switch causes the system to reapply all settings in all GPOs scoped to the user or computer. Some policy settings require a logoff or reboot before they actually take effect. The /logoff and /boot switches of GPUpdate cause a logoff or reboot, respectively. You can use these switches when you apply settings that require a logoff or reboot.

So, the command that will cause a total refresh application, and (if necessary) reboot and logon to apply updated policy settings is:

```
gpupdate /force /logoff /boot
```

In Windows 2000 Server, the Secedit.exe command was used to refresh policy, so you might encounter a mention of the Secedit.exe command on the exam.

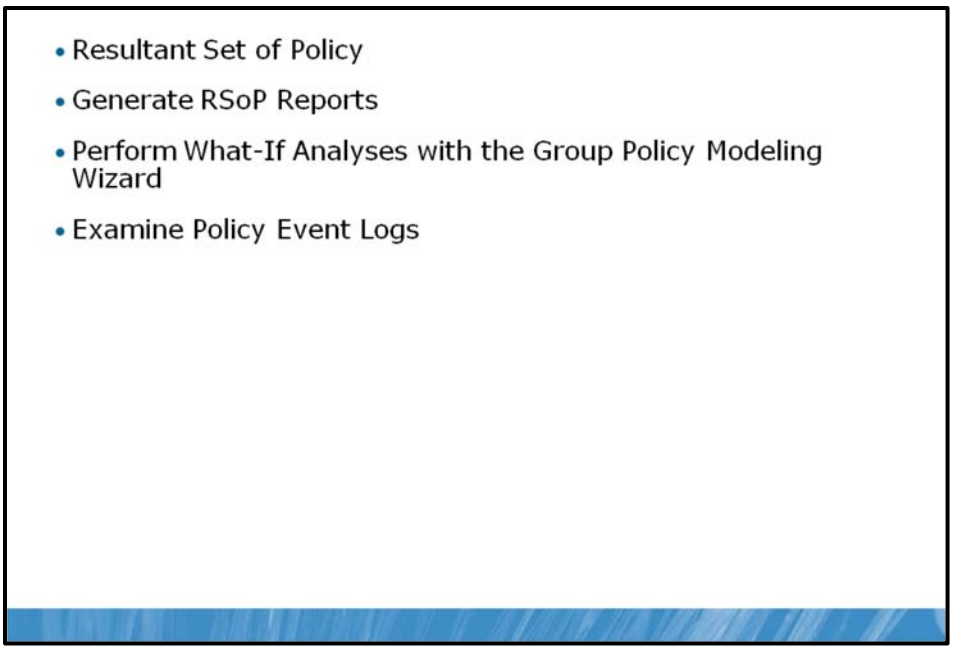
### Most CSEs Do Not Reapply Settings if the GPO Has Not Changed

Remember that most CSEs apply settings in a GPO only if the GPO version has changed. This means if a user can change a setting that was originally specified by Group Policy, the setting will not be brought back into compliance with the settings specified by the GPO until the GPO changes. Luckily, most policy settings cannot be changed by a nonprivileged user. However, if a user is an administrator of their computer, or if the policy setting affects a part of the registry or of the system that the user has permissions to change, this could be a real problem.

You have the option of instructing each CSE to reapply the settings of GPOs even if the GPOs have not been changed. Processing behavior of each CSE can be configured in the policy settings found in Computer Configuration\Administrative Templates\System\Group Policy.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 5
# Troubleshoot Policy Application


• Resultant Set of Policy
• Generate RSoP Reports
• Perform What-If Analyses with the Group Policy Modeling Wizard
• Examine Policy Event Logs

With the interaction of multiple settings in multiple GPOs scoped by using a variety of methods, Group Policy application can be complex to analyze and understand. Therefore, you must be equipped to effectively evaluate and troubleshoot your Group Policy implementation, identify potential problems before they arise, and solve unforeseen challenges. Microsoft Windows provides two tools that are indispensible for supporting Group Policy, Resultant Set of Policy (RSoP) and the Group Policy Operational Logs. In this lesson, you will explore the use of these tools in both proactive and reactive troubleshooting and support scenarios.

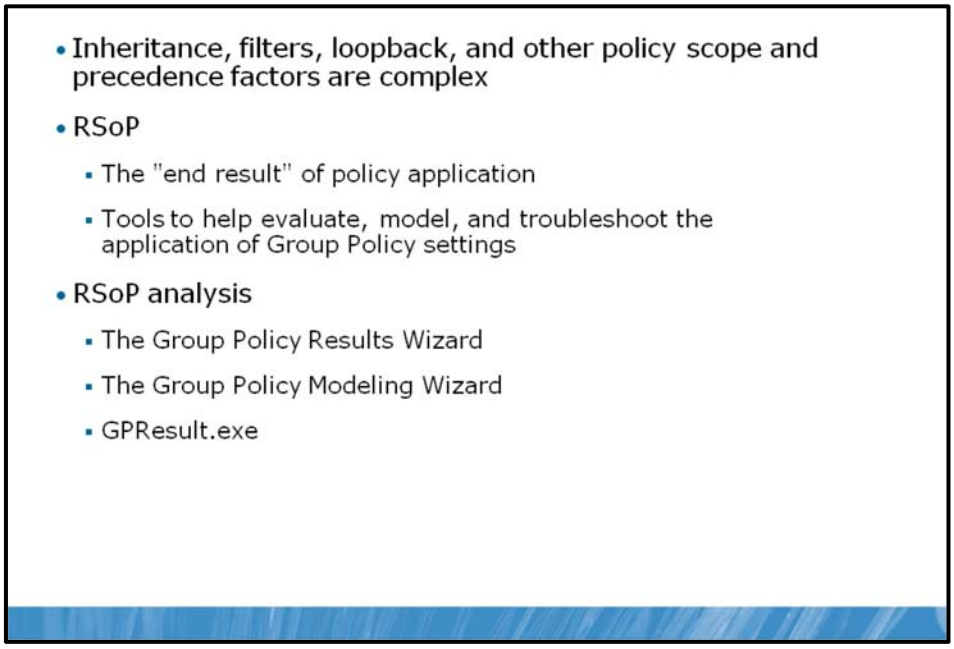
## Objectives

After completing this lesson, you will be able to:

- Analyze the set of GPOs and policy settings that have been applied to a user or computer.
- Proactively model the impact of Group Policy or Active Directory changes on the Resultant Set of Policy (RSOP).
- Locate the event logs containing Group Policy–related events.

MCT USE ONLY. STUDENT USE PROHIBITED

## Resultant Set of Policy


• Inheritance, filters, loopback, and other policy scope and precedence factors are complex
• RSoP
▪ The "end result" of policy application
▪ Tools to help evaluate, model, and troubleshoot the application of Group Policy settings
• RSoP analysis
▪ The Group Policy Results Wizard
▪ The Group Policy Modeling Wizard
▪ GPResult.exe

In Lesson 4, you learned that a user or computer can be within the scope of multiple GPOs. Group Policy inheritance, filters, and exceptions are complex, and it's often difficult to determine which policy settings will apply.

RSoP is the net effect of GPOs applied to a user or computer taking into account GPO links, exceptions, such as Enforced and Block Inheritance, and application of security and WMI filters.

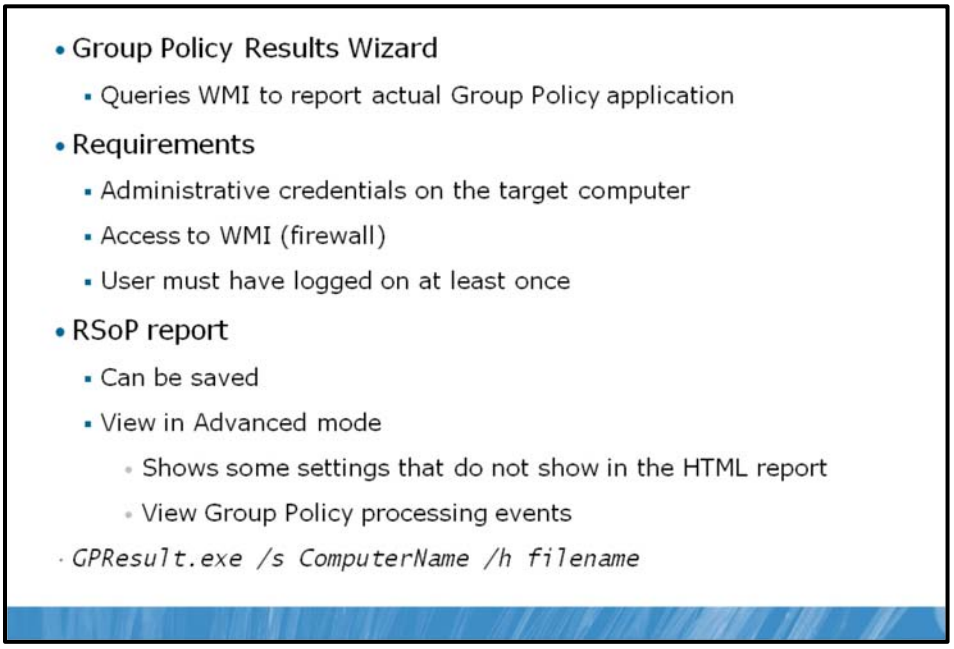
RSoP is also a collection of tools that help you evaluate, model, and troubleshoot the application of Group Policy settings. RSoP can query a local or remote computer and report back the exact settings that were applied to the computer and to any user who has logged on to the computer. RSoP can also model the policy settings that are anticipated to be applied to a user or computer under a variety of scenarios, including moving the object between OUs or sites or changing the object's group membership. With these capabilities, RSoP can help you manage and troubleshoot conflicting policies.

Windows Server 2008 provides the following tools for performing RSoP analysis:

- The Group Policy Results Wizard
- The Group Policy Modeling Wizard
- GPResult.exe

MCT USE ONLY. STUDENT USE PROHIBITED

## Generate RSoP Reports


• Group Policy Results Wizard
▪ Queries WMI to report actual Group Policy application
• Requirements
▪ Administrative credentials on the target computer
▪ Access to WMI (firewall)
▪ User must have logged on at least once
• RSoP report
▪ Can be saved
▪ View in Advanced mode
◦ Shows some settings that do not show in the HTML report
◦ View Group Policy processing events
GPResult.exe /s ComputerName /h filename

To help you analyze the cumulative effect of GPOs and policy settings on a user or computer in your organization, the GPMC includes the Group Policy Results Wizard. If you want to understand exactly which policy settings have applied to a user or a computer, and why, the Group Policy Results Wizard is the tool to use.

The Group Policy Results Wizard can reach into the WMI provider on a local or remote computer running Window Vista, Windows XP, Windows Server 2003, Windows Server 2008, or Windows 7. The WMI provider can report everything there is to know about the way Group Policy was applied to the system. It knows when processing occurred, which GPOs were applied, which GPOs were not applied and why, errors that were encountered, and the exact policy settings that took precedence and their source GPO.

There are several requirements for running the Group Policy Results Wizard, as follows:

- You must have administrative credentials on the target computer.
- The target computer must be running Windows XP or newer. The Group Policy Results Wizard cannot access Windows 2000 systems.
- You must be able to access WMI on the target computer. This means it must be powered on, connected to the network, and accessible through ports 135 and 445.

**Note** Performing RSoP analysis by using Group Policy Results Wizard is just one example of remote administration. To perform remote administration, you may need to configure inbound rules for the firewall used by your clients and servers.

- The WMI service must be started on the target computer.
- If you want to analyze RSoP for a user, that user must have logged on at least once to the computer. It is not necessary for the user to be currently logged on.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

After you have ensured that the requirements are met, you are ready to run an RSoP analysis.

To run an RSoP report, right-click **Group Policy Results** in the GPMC console tree and then click **Group Policy Results Wizard**.

The wizard prompts you to select a computer. It then connects to the WMI provider on that computer and provides a list of users that have logged on to it. You can then select one of the users or opt to skip RSoP analysis for user configuration policies.

The wizard produces a detailed RSoP report in a dynamic HTML format. If Internet Explorer Enhanced Security Configuration is set, you will be prompted to allow the console to display the dynamic content. You can expand or collapse each section of the report by clicking the Show or Hide link, or by double-clicking the heading of the section.

The report is displayed on three tabs:

- **Summary.** The **Summary** tab displays the status of Group Policy processing at the last refresh. You can identify information that was collected about the system, the GPOs that were applied and denied, security group membership that might have affected GPOs filtered with security groups, WMI filters that were analyzed, and the status of CSEs.
- **Settings.** The **Settings** tab displays the resultant set of policy settings applied to the computer or user. This tab shows you exactly what has happened to the user through the effects of your Group Policy implementation. A tremendous amount of information can be gleaned from the Settings tab, but some data isn't reported, such as IPSec, wireless, and disk quota policy settings.
- **Policy Events.** The **Policy Events** tab displays Group Policy events from the event logs of the target computer.

After you have generated an RSoP report with the Group Policy Results Wizard, you can right-click the report to rerun the query, print the report, or save the report as either an XML file or an HTML file that maintains the dynamic expanding and collapsing sections. Both file types can be opened with Internet Explorer, so the RSoP report is portable outside the GPMC.

If you right-click the node of the report itself, under the Group Policy Results folder in the console tree, you can switch to Advanced View. In Advanced View, RSoP is displayed by using the RSoP snap-in, which exposes all applied settings, including IPSec, wireless, and disk quota policies.

## Generate RSoP Reports with GPResult.exe

The GPResult.exe command is the command-line version of the Group Policy Results Wizard. GPResult taps into the same WMI provider as the wizard, produces the same information and, in fact, enables you to create the same graphical reports. GPResult runs on Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008, and Windows 7. Windows 2000 includes a GPResult.exe command, which produces a limited report of Group Policy processing, but is not as sophisticated as the command included in later versions of Windows.

When you run the **GPResult** command, you are likely to use the following options.

```
/scomputername
```

This option specifies the name or IP address of a remote system. If you use a dot (.) as the computer name, or do not include the /s option, the RSoP analysis is performed on the local computer.

```
/scope [user | computer]
```

This displays RSoP analysis for user or computer settings. If you omit the /scope option, RSoP analysis includes both user and computer settings.

```
/userusername
```

This specifies the name of the user for which RSoP data is to be displayed.

```
/r
```

This option displays a summary of RSoP data.

```
/v
```

This option displays verbose RSoP data, which presents the most meaningful information.

```
/z
```

This displays super verbose data, including the details of all policy settings applied to the system. Often, this is more information than you will require for typical Group Policy troubleshooting.

```
/udomain\user/ppassword
```

This provides credentials that are in the Administrators group of a remote system. Without these credentials, GPResult runs by using the credentials with which you are logged on.

```
[/x | /h] filename
```

This option saves the reports in the XML or HTML format. These options are available in Windows Vista SP1 and later, Windows Server 2008 and later, and Windows 7.

### Troubleshoot Group Policy with the Group Policy Results Wizard and GPResult.exe

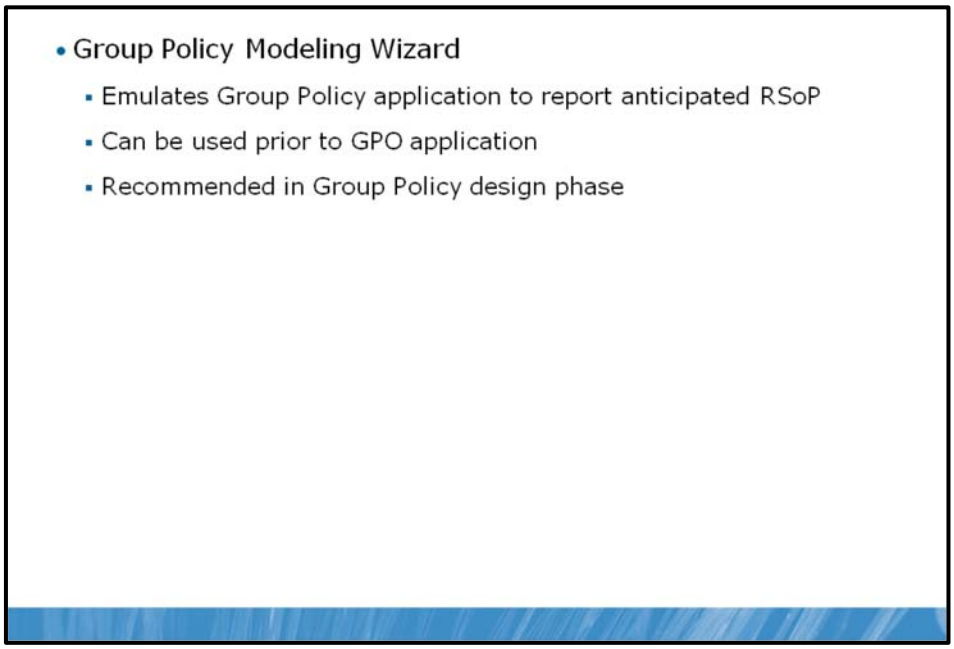
As an administrator, you will likely encounter scenarios that require Group Policy troubleshooting. You might need to diagnose and solve problems, including the following:

- GPOs are not being applied at all.
- The resultant set of policies for a computer or user is not what was expected.

The Group Policy Results Wizard and GPResult.exe will often provide the most valuable insight into Group Policy processing and application problems. Remember that these tools examine the WMI RSoP provider to report exactly what happened on a system. Examining the RSoP report will often point you to GPOs that are scoped incorrectly or policy processing errors that prevented the application of GPO settings.

MCT USE ONLY. STUDENT USE PROHIBITED

## Perform What-If Analyses with the Group Policy Modeling Wizard


Group Policy Modeling Wizard
Emulates Group Policy application to report anticipated RSoP
Can be used prior to GPO application
Recommended in Group Policy design phase

If you move a computer or user between sites, domains, or OUs, or change its security group membership, the GPOs scoped to that user or computer will change. Therefore, the RSoP for the computer or user will be different. The RSoP will also change if slow link or loopback processing occurs, or if there is a change to a system characteristic that is targeted by a WMI filter.

Before you make any of these changes, you should evaluate the potential impact to the RSoP of the user or computer. The Group Policy Results Wizard can perform RSoP analysis only on what has actually happened. To predict the future and to perform what-if analyses, you can use the Group Policy Modeling Wizard.

To perform Group Policy Modeling, right-click the Group Policy Modeling node in the GPMC console tree, click Group Policy Modeling Wizard, and then perform the steps in the wizard.

Modeling is performed by conducting a simulation on a domain controller, so you are first asked to select a domain controller that is running Windows Server 2003 or later. You do not need to be logged on locally to the domain controller, but the modeling request will be performed on the domain controller. You are then asked to specify the settings for the simulation.

- Select a user or computer object to evaluate, or specify the OU, site, or domain to evaluate.
- Choose whether slow link processing should be simulated.
- Specify to simulate loopback processing and, if so, choose Replace or Merge mode.
- Select a site to simulate.
- Select security groups for the user and for the computer.
- Choose which WMI filters to apply in the simulation of user and computer policy processing.

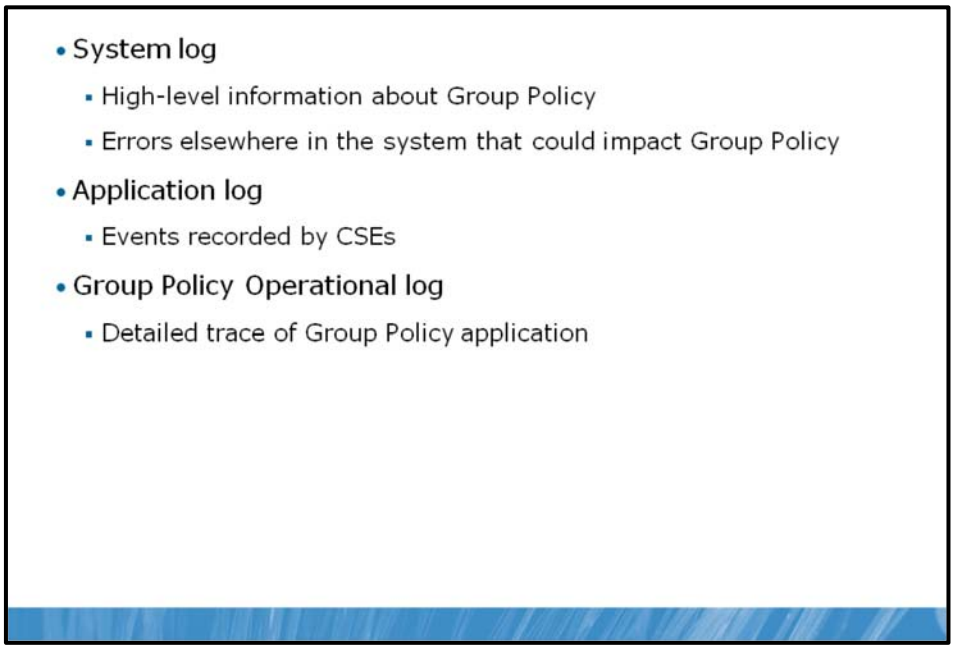
When you have specified the settings for the simulation, a report is produced that is very similar to the Group Policy Results report discussed earlier. The Summary tab shows an overview of which GPOs will be

MCT USE ONLY. STUDENT USE PROHIBITED

processed, and the Settings tab details the policy settings that will be applied to the user or computer. This report, too, can be saved by right-clicking it and choosing Save Report.

MCT USE ONLY. STUDENT USE PROHIBITED

## Examine Policy Event Logs


• System log
▪ High-level information about Group Policy
▪ Errors elsewhere in the system that could impact Group Policy
• Application log
▪ Events recorded by CSEs
• Group Policy Operational log
▪ Detailed trace of Group Policy application

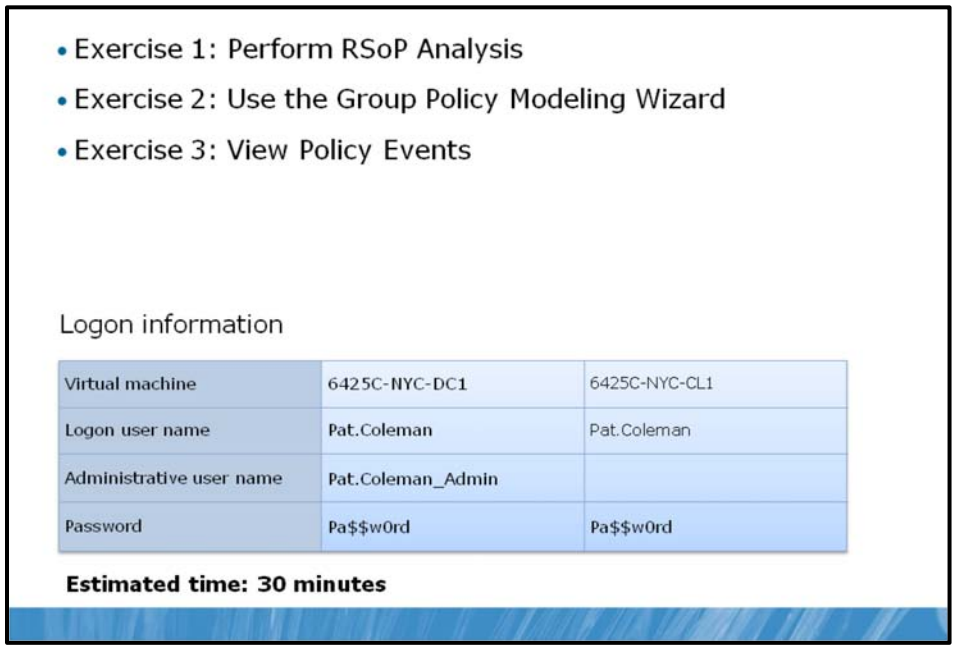
Windows Vista, Windows Server 2008, and Windows 7 improve your ability to troubleshoot Group Policy not only with RSoP tools, but also with improved logging of Group Policy events.

- In the System log, you will find high-level information about Group Policy, including errors created by the Group Policy client when it cannot connect to a domain controller or locate GPOs.
- The Application log captures events recorded by CSEs.
- A new log, called the Group Policy Operational Log, provides detailed information about Group Policy processing.

To find Group Policy logs, open the Event Viewer snap-in or console. The System and Application logs are in the Windows Logs node. The Group Policy Operational Log is found in Applications And Services Logs\Microsoft \Windows\GroupPolicy\Operational.

MCT USE ONLY. STUDENT USE PROHIBITED

# Lab C: Troubleshoot Policy Application




## Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **6425C-NYC-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
   - User name: **Pat.Coleman**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
5. Start 6425C-NYC-CL1. Log on to NYC-CL1 as Pat.Coleman with the password of Pa$$w0rd.

## Lab Scenario

You are responsible for administering and troubleshooting the Group Policy infrastructure at Contoso, Ltd. You want to evaluate the resultant set of policies for users in your environment to ensure that the Group Policy infrastructure is healthy, and that all policies are applied as they were intended.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 1: Perform RSoP Analysis

In this exercise, you will evaluate the resultant set of policy by using both the Group Policy Results Wizard and the GPResults command.

The main tasks for this exercise are as follows:

1. Refresh Group Policy.
2. Create a Group Policy results RSoP report.
3. Analyze RSoP with GPResults.

### ▶ Task 1: Refresh Group Policy.

1. On NYC-CL1, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. Run the **gpupdate /force** command. After the command has completed, make a note of the current system time, which you will need to know for a task later in this lab.
3. Restart NYC-CL1 and wait for it to restart before proceeding with the next task.

### ▶ Task 2: Create a Group Policy results RSoP report.

1. On NYC-DC1, run the **Group Policy Management** console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. Use the **Group Policy Results Wizard** to run an RSoP report for **Pat.Coleman** on NYC-CL1.
3. Review **Group Policy Summary** results. For both user and computer configuration, identify the time of the last policy refresh and the list of allowed and denied GPOs. Identify the components that were used to process policy settings.
4. Click the **Settings** tab. Review the settings that were applied during user and computer policy application, and identify the GPO from which the settings were obtained.
5. Click the **Policy Events** tab, and locate the event that logs the policy refresh you triggered with the **GPUpdate** command in Task 1.
6. Click the **Summary** tab, right-click the page, and choose **Save Report**. Save the report as an HTML file to drive D with a name of your choice. Then open the RSoP report from drive D.

### ▶ Task 3: Analyze RSoP with GPResults.

1. Log on to NYC-CL1 as **Pat.Coleman_Admin** with the password **Pa$$w0rd**.
2. Run the command prompt with administrative credentials.
3. Type **gpresult /r** and press Enter.

   RSoP summary results are displayed. The information is very similar to the Summary tab of the RSoP report produced by the Group Policy Results Wizard.
4. Type **gpresult /v** and press Enter.

   A more detailed RSoP report is produced. Notice that many of the Group Policy settings applied by the client are listed in this report.
5. Type **gpresult /z** and press Enter.

   The most detailed RSoP report is produced.

6. Type **gpresult /h:"%userprofile%\Desktop\RSOP.html"** and press Enter.

   An RSoP report is saved as an HTML file to your desktop.

7. Open the saved RSoP report from your desktop.

8. Compare the report, its information, and its formatting with the RSoP report you saved in the previous task.

**Results:** In this exercise, you learned how to do a resultant set of policy in two ways, using a wizard and from the command line.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 2: Use the Group Policy Modeling Wizard

Before you roll out the Conference Room Policies GPO for production, you want to evaluate the effect it will have on users who log on to conference room computers. In this exercise, you will use the Group Policy Modeling Wizard to model the resultant set of policies applied to a user, Mike Danseglio, if he were to log on to a conference room computer, NYC-CL1.

The main task for this exercise is as follows:

- Perform Group Policy results modeling.

**Note** This task requires greater level of detail in the high level steps compare to other tasks in the module. .

### ▶ Task 1: Perform Group Policy results modeling.

1. Switch to **NYC-DC1**.
2. In the Group Policy Management console tree, expand **Forest:Contoso.com**, and then click **Group Policy Modeling**.
3. Right-click **Group Policy Modeling**, and then click Group Policy Modeling Wizard.

   The **Group Policy Modeling Wizard** appears.
4. Click **Next**.
5. On the **Domain Controller Selection** page, click **Next**.
6. On the **User And Computer Selection** page, in the **User Information** section, click **User**, and then click **Browse**.

   The **Select User** dialog box appears.
7. Type **Mike.Danseglio** and then press Enter.
8. In the **Computer Information** section, click the **Computer** option button, and then click **Browse**.

   The **Select Computer** dialog box appears.
9. Type **NYC-CL1** and then press Enter.
10. Click **Next**.
11. On the **Advanced Simulation Options** page, select the **Loopback Processing** check box, and then click **Merge**.

    Even though the **Conference Room Polices** GPO specifies loopback processing, you must instruct the **Group Policy Modeling Wizard** to consider loopback processing in its simulation.
12. Click **Next**.
13. On the **Alternate Active Directory Paths** page, click the **Browse** button next to **Computer location**.

    The **Choose Computer Container** dialog box appears.
14. Expand **contoso.com** and **Kiosks**, and then click **Conference Rooms**.

    You are simulating the effect of **NYC-CL1** as a conference room computer.
15. Click **OK**.

16. Click **Next**.
17. On the **User Security Groups** page, click **Next**.
18. On the **Computer Security Groups** page, click **Next**.
19. On the **WMI Filters for Users** page, click **Next**.
20. On the **WMI Filters for Computers** page, click. **Next**.
21. Review your settings on the **Summary of Selections** page, and then click **Next**.
22. Click **Finish**.
23. On the **Summary** tab, scroll to and expand, if necessary, **User Configuration, Group Policy Objects**, and **Applied GPOs**.
24. Check whether the **Conference Room Policies** GPO apply to Mike Danseglio as a User policy when he logs on to **NYC-CL1if NYC-CL1**is in the Conference Rooms OU.

    If not, check the scope of the **Conference Room Policies** GPO. It should be linked to the **Conference Rooms** OU with security group filtering that applies the GPO to the **Authenticated Users** special identity. You can right-click the modeling query to rerun the query. If the GPO is still not applying, try deleting and re-building the **Group Policy Modeling** report, and be very careful to follow each step precisely.
25. Click the **Settings** tab.
26. Scroll to, and expand if necessary, **User Configuration**, **Policies**, **Administrative Templates** and **Control Panel/Personalization**.
27. Confirm that the screen saver timeout is 2,700 seconds (45 minutes), the setting configured by the **Conference Room Policies** GPO that overrides the 10-minute standard configured by the **CONTOSO Standards** GPO.

**Results:** In this exercise, you used the Group Policy Modeling Wizard to confirm that the Conference Room Policies GPO in fact applies its settings to users logging on to conference room computers.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Exercise 3: View Policy Events

As a client performs a policy refresh, Group Policy components log entries to the Windows event logs. In this exercise, you will locate and examine Group Policy–related events.

The main task for this exercise is as follows:

- View policy events.

### ▶ Task 1: View policy events.

1. On NYC-CL1**,** where you are logged on as **Pat.Coleman_Admin**, run Event Viewer as an administrator.
2. Locate and review **Group Policy** events in the **System** log.
3. Locate and review **Group Policy** events in the **Application** log.

**Note** Depending on how long the virtual machine has been running, you may not have any Group Policy Events in the application log.

In the **Group Policy Operational** log, locate the first event related in the **Group Policy** refresh you initiated in Exercise 1, with the **GPUpdate** command. Review that event and the events that followed it.

**Results:** In this exercise, you identified Group Policy events in the event logs.

### ▶ To prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start Hyper-V Manager.
2. Right-click **6425C-NYC-DC1** in the **Virtual Machines** list, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for **6425C-NYC-CL1**.

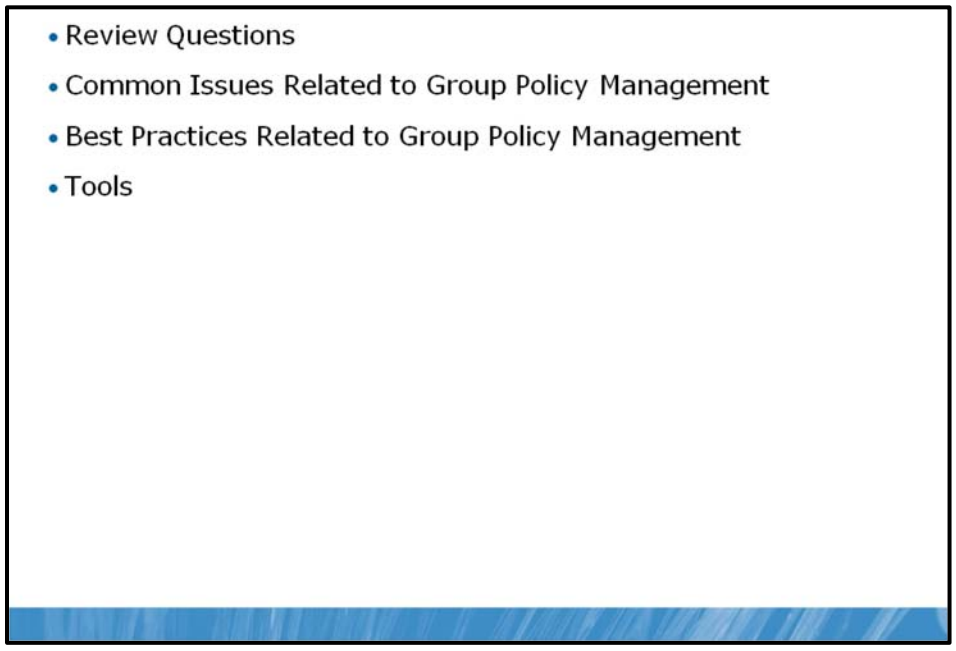
## Lab Review Questions

**Question:** In which situations have you used RSoP reports to troubleshoot Group Policy application in your organization?

**Question:** In which situations have you used, or could you anticipate using, Group Policy modeling?

**Question:** Have you ever diagnosed a Group Policy application problem based on events in one of the event logs?

# Module Review and Takeaways


• Review Questions
• Common Issues Related to Group Policy Management
• Best Practices Related to Group Policy Management
• Tools

## Review Questions

1. You have assigned a logon script to an OU via Group Policy. The script is located in a shared network folder named Scripts. Some users in the OU receive the script, whereas others do not. What might be the possible causes?
2. What GPO settings are applied across slow links by default?
3. You need to ensure that a domain level policy is enforced, but the Managers global group needs to be exempt from the policy. How would you accomplish this?

## Common Issues Related to Group Policy Management

| Issue | Troubleshooting tip |
|---|---|
| Group Policy settings are not applied to all users or computers in OU where GPO is applied | |
| Group policy settings sometimes need two restarts to apply | |

## Best Practices Related to Group Policy Management

- Name Group Policy objects, so you can easily identify them by name
- Apply Group Policy Object as high as possible in AD DS hierarchy
- Use Block Inheritance and Enforced options only when really necessary
- Make comments on GPO settings

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Group policy reporting RSoP | Reporting information about the current policies being delivered to clients. | Group Policy Management Console |
| GPResult | A command-line utility that displays RSoP information. | Command-line utility |
| GPUpdate | Refreshing local and AD DS-based Group Policy settings. | Command-line utility |
| Dcgpofix | Restoring the default Group Policy objects to their original state after initial installation. | Command-line utility |
| GPOLogView | Exporting Group Policy-related events from the system and operational logs into text, HTML, or XML files. For use with Windows Vista, Windows 7, and later versions. | Command-line utility |
| Group Policy Management scripts | Sample scripts that perform a number of different troubleshooting and maintenance tasks. | |